Topic 11

Responding to a Breach

Dr Diarmuid Ó Briain

Version: 3.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

This page is intentionally blank

1 Objectives

By the end of this topic, you will be able to:

- Define a breach and explain why it is important to respond to it quickly and effectively.
- Describe the different types of breaches and their impact on individuals, businesses, and organisations.
- Identify the key steps involved in the breach response lifecycle.
- Explain the importance of having a Cyber Security Incident Response Plan (CSIRP) in place.
- Discuss the different roles and responsibilities involved in a breach response.
- Identify best practices for communicating with internal and external stakeholders during a breach response.

2 Introduction

Data breaches occur daily with many global organisations falling victim regularly and they're a problem for everyone not just Security professionals. The rapid increase and the sheer amount of interconnected systems has created unparalleled opportunities to compromise records and steal information. These cyber crimes are mounting not only in number but severity and the total amount of information compromised is overwhelming. Information Security professionals must have a sound and current appreciation for the range of potential criminal acts and actors and how to respond in the event of a breach to their systems. Any information system may be the target of such a criminal act or used as a foothold to infiltrate systems. For many organisations who have suffered breaches this could be their customer network or even an Heating, Ventilation, and Air Conditioning (HVAC) system. Whether the attacks are for profit, fame, or just to cause chaos the result is the same. An organisation will be judged more by their response to a breach and not necessarily the scope of the breach. Attackers come in all shapes and sizes and coupled with the steadily improving capabilities of the malicious actors to target information and infrastructure, today's Information and Security professional faces an evermore difficult task of securing their environment from compromise.

3 Immersive Exercise (Part 1) – Scenario develops

3.1 The Phone Rings

So far, this is just an average night at Hologram Keys. They design and produce wireless keys and access cards for various types of high-end vehicles including electric cars, helicopters, and private aircraft. They use a co-located Cloud Service Management to house and maintain many systems as well as store data, including their intellectual property and customer information, which is highly sensitive based on the net worth of their average customer. Their design IP is unparalleled as an industry leader and access to the IP could open vulnerabilities like spoofed access keys to the transportation of the world's elite. In the past, this had made Hologram a target for black hat hackers that sell stolen data on the dark web. Tonight, like any other night, there is minimal staff on the graveyard shift and monitoring is largely automated. The analysts are reviewing logs, creating backups, and performing other routine tasks. A fresh pot of coffee is on. It seems like everything is running smoothly, but that is all about to change.

Mary, an analyst notices an alert. She thinks to herself, 'This does not look right.' She quickly checks some logs and verifies the result. It could be harmless, but it definitely needs to be checked out. It could be the tip of a very dangerous iceberg. Miles away there is a dark home at the end of the cul-de-sac. Everyone inside is sleeping peacefully. Well, almost everybody. Your phone rings. You fumble around your bedside table, grasping at anything that feels remotely like a cell phone. You've found it and you know that number. Though there's never been a significant incident - nothing with lasting damage anyway - you cannot help but feel anxious whenever that number appears. Your heart drops to your stomach and you barely whisper 'This can't

be good' above the shrill ringtone echoing around the quiet dark room. You pick up the phone and with as much calm as you can muster you say hello. You turn on the light and sit up on the edge of the bed listening to Mary on the other end of the line from the company Security Operations Centre (SOC). After a few security questions asked and answered, your identity is verified and you're told unfortunate news. "*Sorry to bother you in the middle of the night, but we've had what appears to be a major incursion.*" Any grogginess that you once felt a minute ago vanished. She continues, "*There are some logs coming from the Security Event and Incident Management system, (SEIM), that shows a user that has moved laterally across systems in an abnormal way. We cannot seem to see a clear path of the user's movement. There is an issue with the logs, almost like someone tried to scrub them, but we've connected the dots on at least two networks and it does not look good. We will need help to get to the bottom of this. What should we do?*"

3.2 Definitions and Types

At a high level, the definition of a breach may slightly vary from organisation to organisation and across different legal frameworks and local legislation. In it is purest form, a breach has occurred if there has been unauthorised access to information systems. What is a data breach? Although as mentioned previously, there are various conflicting definitions of what constitutes a breach, it is important to understand the differences between events, incidents, and breaches. They can be broken down as follows.

- **A security event**: is a record of an action taken against an information system that alters the system's state. An organisation can have millions of events that occur throughout a date.
- **A security incident**: is an event or series of correlated events that indicate that a potential violation of some control or policy has occurred. This is a smaller subset of security events.
- **A security breach**: is defined as unauthorised access that violates the confidentiality, integrity, or availability of an information asset in the form of unintentional access, destruction, or manipulation of an information asset.

When it comes to security breaches, there are different types. Each with a different type of impact on people and businesses. Here is a sample of the most common types along with real world examples.

With regards to personal information, we can define it as an individual's first name or first initial, and last name in combination with one or more of the following data: Social Security Number, Driver's License number or state identification card number, financial account number, credit or debit card number with personal identification number, such as an access code, security codes, or password that would permit access to an individual's financial account, medical or health insurance information, or a username or email address in combination with a password or security question and answer that would permit access to an online account.

3.3 Breach Sources

Sources of breaches include the following:

- Social engineering
- Network or system intrusion
- Malware Viruses
- Advanced persistent threats
- Malicious insider
- Removable media
- Improper usage
- Human Error
- 3rd party on integrated systems

3.3.1 Attack vector sources

- 76% breaches were financially motivated.
- 73% of all cyber attacks were carried out by outsiders.
- 28% of all cyber attacks were carried out by insiders.

3.4 Why This Matters?

A cybersecurity breach can very quickly affect your organisation and put your data and business at risk. Regardless of how many technological controls are in place, no defence is ever fool proof. Understanding the fundamentals of a breach and knowing how to respond to it methodically will help minimise data loss and destruction of business services and potential lost revenue. Time is of the essence when it comes to data breaches and having a plan and concrete processes will allow response teams to take action swiftly. A proactive stance is the best place to be. And solid planning has proven to reduce the impact of a breach to an organisation significantly.

3.5 Introducing the Response Lifecycle

it is only a matter of when, not if, that a security incident or breach, of an organisation will happen. Preparation with tools is essential, but understanding the life cycle of a breach, can help stop the bleeding quickly and efficiently. The life cycle is broken down into four phases, and serves to provide a basis for teams to take responsive measures. In the modules ahead, we will explore the different stages in depth, and offer strategies which will help you better prepare to respond to a breach. The four phases are;

1. Detection and analysis
2. Investigation, containment, and mitigation
3. Recovery and notification
4. Post-incident review

3.6 Detection and Analysis

The detection and analysis phase revolves around the process of identifying various security incidents, breaches, vulnerabilities and more. Being able to discover a potential incident before it escalates is crucial. In fact, 68% of breaches took several months or longer before they were discovered. Having documented processes and thorough analysis techniques play a significant role in quickly and efficiently identifying a breach. The NIST Framework provides some guidance when it comes to this phase and recommends breaking it down into two groups;

- **Precursors**: Signify that an incident may occur in the future for example, when you receive alerts that several web servers are being scanned by a vulnerability scanner.
- **Indicator**: Provides evidence of a current or previous incident. A typical example is when an antivirus solution triggers alerts when a host has been infected with malware. Many security tools are capable of flagging indicators and some tools even have the capability to conduct an initial analysis. Keep these concepts in mind when developing processes around detection and analysis for your organisation.

3.7 Investigation, Containment, and Mitigation

Investigations are all about gathering evidence to determine a root cause before taking actions to contain a breach. This can be challenging, however, as breaches are dynamic in nature, and tracing back to the root cause can be arduous. Documentation is a critical component of this phase, and you'll want to create a record of all the details and evidence about the breach. This will be useful should your organisation choose to engage law enforcement or take legal action against the perpetrator. In addition, a chain of custody should be created so that evidence is always accounted for, especially when transferred to different individuals. Containing a breach before it becomes widespread and causes significant damage is critical.

Damage limitation is the goal. Ultimately, you need to be able to minimise the risk of further impact to your organisation while keeping business processes functional where possible. it is a challenging balancing act, but one that is managed with the right strategies in place. Understand that strategies are dependent on the type of incident. For instance, you wouldn't respond to a DDoS attack the same way you would a data breach involving Personally Identifiable Information (PII). Mitigation comes down to purging all elements related to the breach, including any artefacts left behind by the perpetrator. This is a critical step to ensure all attack vectors have been closed, but depending on the scale of the breach or attack, it may take some time. Prioritise your remediation process and take a phased approach, so you can address areas of concern based on risk to your environment. Documentation is once more relevant here, as you record the steps taken to address each issue caused by the breach. When working to contain and mitigate a breach, remember to remain calm. it is easy to get carried away and overwhelmed by the situation, but taking things one step at a time will ensure you are better prepared to respond to a breach.

3.8 Recovery and Notification

Now, let's talk about the recovery phase. Here, the focus is around restoring affected systems to its normal production status. Recovery can be considered complete when the businesses return to a fully operational state, though there may be changes to the design and configuration of your environment, such as adding additional security controls and monitoring. Testing and validation of compromised systems will ensure that they are in a clean state. It is imperative that this is done thoroughly before bringing them back into your production network. Validation should also occur from a business perspective to ensure all functionality is working as expected. Notification is a component of incident response that affects many groups within an organisation. And it is often not thorough enough, or left out entirely. it is imperative that a communication plan is in place that details which individuals should be notified at each phase of the response life cycle. Some of this can be automated with tools explicitly designed for incident response. In addition, notification is not only relevant to internal stake holders, but external ones as well, including the media, regulators and government entities. We will discuss this in greater detail in the modules ahead. While notification is the phase of its own, it should be practised in each phase of the response life cycle. Clear and effective communication is a core driver in the timeliness of responding to a breach.

Marriott's breach response is so bad, security experts are filling in the gaps — at their own expense

3.9 Post-Incident Review

The post-incident review, is just as critical as the other phases in the response life cycle. This is an excellent opportunity for all the teams and individuals involved, to understand what happened, what actions were taken, and gauge the effectiveness of their response. it is also a chance to identify positive takeaways, as well as areas of improvement for a wide range of activities. A post-incident report should also be completed at this time, and signed off by appropriate personnel in the organisation, and stored in a secure repository. This serves as a reference for handling similar incidents in the future, and should cover all activities taken in response to the incident.

Yahoo Execs 'Ignored' Security Team Over 2014 Breach

3.10 Cyber Security Incident Response Plan (CSIRP)

You may have seen the acronym CSIRP in various media relating to cyber security before. It stands for Cyber Security Incident Response Plan, and it is an important document containing your organisation's official programme on dealing with breaches and attacks. Having a comprehensive step-by-step plan ensures your company is prepared to contain and mitigate any security incident quickly and effectively. Your plan will also establish how you communicate to stakeholders across all business units from incident conception to resolution. Success, however, is dependent on ensuring it is easily accessible for all core team members and put into practice through playbooks or tabletop exercises. This will allow the team to assess the various tools, processes, and general aptitude in responding to various incidents, from

a strategic and technical standpoint. it is recommended that you review your plan at least twice a year, to ensure details such as contact information, and reporting methods are up to date.

3.10.1 Components of CSIRP

Common sections of a CSIRP (non-exhaustive list)

- **Introduction**: This is the first thing that people will see, and sets the tone for the plan.
- **Plan overview and objectives**: This provides the context, the business, and outlines the high-level who, what, where, when, and why of the plan.
- **Scope**: This covers what is and isn't covered in the plan.
- **Roles, responsibilities and team definitions**: Team members have a mission to prevent a serious loss of profits, public confidence, or information assets, by providing an immediate, effective, and skillful response to any cyber incident. This portion outlines the specific personnel assigned to roles and expectations around outcomes.
- **Definitions**: This sections is often used to describe technical terms that may be used within the plan, and provide definitions as to what an event, incident and breach means to an organisation.
- **Plan structure/Methodology**: This lays out the framework for approaching and responding to an incident.
- **Contact List**: This contains a list of all key personnel who should be contacted in the event of an incident.
- This list should contain primary and secondary contacts for each team involved.
- **Notifications**: Contains the teams or groups that are part of the communications plan, and outlines who will receive updates about an ongoing incident and how often.
- **Incident declaration**: Protocols defined for declaring an incident and activating the plan.
- **Checklists and process**: Guides for completing particular tasks, such as process flows, checklists, and specific operations performed during a response.
- **Incident severity matrix**: A definition of your organisation's incident types and the corresponding activities associated with the severity ratings.

3.10.2 Cyber Security Instant Response Team (CSIRT)

The team’s mission is to prevent a serious loss of profits, public confidence, or information assets by providing an immediate and skilful response to any unexpected event involving computer information systems, networks or databases.

A CSIRT is established to provide a quick and effective and orderly response to cyber security related incidents. The team's mission is to prevent a severe loss of profits, public confidence, or information access by providing an immediate and skilful response to any unexpected event involving computers and information systems, networks, or databases. The team is generally led by a lead incident handler. The lead will be authorised to engage resources as required to manage the incident

effectively and to take appropriate steps deemed necessary to contain, mitigate, and also resolve a breach. Additional responsibilities include reporting findings to executive management and the appropriate authorities as needed. Ultimately, however, all organisational groups have a role to play in the event of a breach, though it all begins with the core team, which is comprised of various IT units. Through your efforts in developing a CSIRT, you will need to build valuable and lasting relationships with the business. No matter the size of your organisation, you will need to depend on people outside of security and IT. These individuals will be critical in maintaining and testing the plan's execution. These may vary from organisation to organisation, but it is an essential factor to understand connections with the business and include them in your CSIRT. Additionally, you can leverage your CSIRT to build new relationships with law enforcement. Your plan should include dealing with criminal misconduct. When developing or updating your plan, it is essential, particularly in a crisis, to know who to contact and how to reach them. Most law enforcement agencies that specialise in cyber crime are eager to provide resources that help you in developing your response plan.

3.11 Building a Breach Response Plan

The Breach Response Plan document and all associated materials are to assist in developing the organisation's plan, so you should consider this document a blueprint and not all-encompassing. Every organisation is different, and these plans may vary greatly from one organisation to another. Start with a template template that will allow you to go through each segment and tailor it to your organisation. Also, depending on the size of your organisation, for example, if you worked for a very large one, your plan may actually be broken down into several different components, so you may have a overall policy-driven document that kind of guides what you're doing with your breach response. You may have a process-oriented document that outlines all the plan processes, and then you may have another document that connects the breach response plan to all your standard operating procedures. So, do what works best for you and your organisation, and if you find yourself looking for additional materials, there's actually a number of standards that you can reference and model your plan from. For example, you can model it based on;

- NIST Special Publication 800-61 information response guide
- ISO 27002 standard of good practice for information security
- ITIL service operation, Incident Management (IM) practice for restoring services as quickly as possible after an incident
- COBIT, Control Objectives for Information and Related Technologies

3.11.1 Introduction

The introduction sets the tone and tenor for the rest of your plan. It provides a executive summary of sorts. The introduction will reflect the culture of your organisation and set the stage for the rest of the content.

3.11.2 Plan objectives

For some, this may be similar to the introduction, or you may even choose to put your objectives in your introduction. No matter where you put them, you need to outline the high-level objectives you hope to accomplish with this plan. Objectives should be clear, actionable, and describe the overall purpose of the document. Basically, you're answering the "why" to the existence of this document. So, some sample objectives could be, "supporting the business recovery efforts being made in the aftermath of an incident," "identifying, containing, and rapidly responding to an incident," "assess and ascertain the severity of the incident quickly and effectively." One other approach that a lot of organisations take in their objectives is to define the value proposition of the plan, basically selling the plan to the business.

3.11.3 Scope in ownership

One thing you want to make sure that you do is adequately scope your document. The scope helps outline the area of responsibility with those involved and basically sets up your guardrails. In particular, for large organisations with multiple business units, sub-organisations, it is important to identify the boundaries for the plan for its effective execution. The scope section will also identify the incident types that will activate the plan, so it is very likely you have many connected documents such as your disaster recovery and business continuity plans. You should use the scope section to define what the plan is and what it isn't, and here, you should define those connections or triggers to other plans and documents.

3.11.4 Ownership

Ownership is key. The owner and their respective backup should be clearly stated in your document. The importance of this cannot be understated and is ultimately going to fall on a single individual or small group of people. Absolutely pertinent to establish accountability and responsibility for the plan, the management of the plan, and the lifecycle of the document. So, just a quick tip: although we haven't explicitly called it out, the beginning of the plan, somewhere, should detail the executive sponsorship and upper management support of the plan. As with all things cyber, having management buy-in and support is going to be key to this plan and any of its associated activities.

3.11.5 Definitions

So, not everyone's going to know what "DDoS" stands for, and you will likely have the internal, external, technical, and non-technical individuals as part of your team. During an emergency, confusion and chaos are not your friends. Therefore, you should take the time to identify terms, acronyms, and portions of the plan that may need definitions. Although you may think your plan is straightforward, a misstep can be costly, especially when dealing with a breach. Again, you may prefer a different order

for how this section appears in your plan, but it is usually a good practice to place definitions in the front, not stuck in an appendix in the back of the document.

3.12 Team definition

This is where the rubber starts to meet the road. Roles and responsibilities need to be explicitly defined and an outline of authority associated with those roles. Clear lines need to be drawn, and your teams need to understand the chain of command. That way, messages aren't crossed or confused when the time of, well, heightened emotions. You'll want to define both your core technical teams as well as those that sit in your various business units. Even if you decide to use titles or roles instead of named individuals, there should be no question of who should be doing what. Time is running against you, and efficiency is key to getting you to the other end of the tunnel.

4 Immersive Exercise (Part 2) – Calling in the CSIRT

You respond, "*Let's call in the team.*" Your heart is beating out of your chest. How big is this? What all did they get access to? Could this just be a mistake? Your mind is racing, but you know the path forward. You reassure yourself, because you know you work for a company that cares about the customers and their employees. And you care, too. There's a Cyber Security Incident Response Plan (CSIRP), in place. You ask Mary to make contact with the Incident Response team. Everyone local should report to HQ. You ask, "*Has there been a sweep of the SOC for unauthorised physical presence? Any keylogging devices or errant USB drives plugged in? We need a complete report of that in the next hour. We also need the War Room set up ASAP. Please help us get the second floor conference room reserved and get the secure video and audio conference set up. Make sure it is encrypted. If someone is on the network, we can't have them listening in.*"

1. Call in the Cyber Security Instant Response Team (CSIRT)
2. Follow the Cyber Security Incident Response Plan (CSIRP)
3. Sweep the SOC for unauthorised physical presence?
4. Establish the War Room.
    - Make sure it is encrypted to prevent eavesdropping.

4.1 Self Test

1. What is a security breach defined as?
   - Record of an action taken against an information system that alters the system's state. An organisation can have millions of events that can occur throughout a day.
   - Event or series of correlated events that indicate that a potential violation of some control or policy has occurred. Security This is a smaller subset of security events.
   - Unauthorised access that violates the confidentiality, integrity, or availability of an information asset in the form of unintentional access, destruction, or manipulation of an information asset.
   - None of the above

   Answer: Unauthorised access that violates the confidentiality, integrity, or availability of an information asset in the form of unintentional access, destruction, or manipulation of an information asset.

2. A precursor is the notion that there is evidence of a current or previous incident, such as an antivirus solution triggering alerts when a host has been infected with malware.

   Answer: False

3. What does the acronym CSIRP stand for?

   Answer: Cyber Security Incident Response Plan

5 Immersive Exercise (Part 3) – The gathering of the CSIRT

5.1 Detection and Analysis

You pull up to the office and step out of your car. Just as soon as your feet hit the pavement, your cell phone is to your ear and you are making a phone call. "*Is everyone on the way? Are you using the cell numbers in the CSIRP?*" The team begins to arrive at HQ within the hour. It is still early, but this is what they have planned and trained for. The office is ablaze with swift footsteps and intense conversation. It is a stark contrast from a few hours earlier when even the smallest noise would have echoed across the room. You are glad the team has been contacted, but you are desperate for any details, any clue as to what happened. You ask Mary if there is any information on the scope so far, but there is no news, and you know it is going to take teamwork to assess this situation, let alone contain and remediate. You thank Mary, hang up, and enter the building. The First Responders have gathered together under your direction as outlined in the CSIRP. You convene a video call and try to get a handle on who knows what so far. You are calm, but you know that time is critical, so you are speaking quickly and deliberately. You are looking for the incident lead from the SOC "*Alright team, we need information, a lot of it, from a lot of places. We need to be sure we have the SOC lead on. You there? Good. After this call please head in so we can coordinate from the War Room. Also, where is that Continuous Security Monitoring (CSM) physical security report? Already sent? Great, let us review that together when you get here. We also need to get in touch with the Senior Security Engineer. Oh no, they are out of the country on vacation?*" There is lots to figure out, and they could still discover this is anomalous, yet benign activity, but they won't know until they do the investigation. You are very worried about the chain of custody. If the wrong person touches the data and the evidence is tainted, you might not have a strong case against a possible intruder.

5.2 Pre-Incident

- People, Process and Technology
- Risk Management and Assessment
- Business Continuity Management

5.2.1 People, Process & Technology

When it comes to security, it always starts with people. it is important to ensure your organisation has fostered a culture of security, and it must start at the top with the C-suite and board of directors to build and manage that culture. In addition, every employee is a gatekeeper of information and holds a responsibility to secure the information they work with. Instilling a culture of security through policy and interactive end user training, will raise awareness and increase the security of your organisation. Some crucial aspects of this is ensuring your employees know how to report any type of suspected security incident, have several methods of reporting, and are praised for doing so. This reinforces the education provided and improves the culture of security. Your organisation should also have a comprehensive security programme. Creating

standard policies, procedures, and processes, serves as guides on behaviour from a security standpoint, specifically around how users interact with company data and systems more securely. They often define the who, what, and why about those behaviours, and help define and foster an organisation security culture. Your security programme should be reviewed and updated at least once a year. Technology's role cannot be understated. All hosts on your network should be updated with the latest patches and secured using standard configurations. Controls such as antivirus and appropriate firewall rules should be in place and configured correctly, along with login capabilities enabled.

- Who
- What
- Why

5.2.2 Risk Management and Assessment

Risk management is core to any security programme, and goes a long way in assisting an organisation in its security hygiene. The scope of this course does not go into the intricacies of building a proper risk management programme, but it is instrumental in preventing cyber breaches. Conducting risk assessments of your network, systems, and applications will provide insight into what threats and vulnerabilities are most relevant and critical, and will help you paint an overall picture of risks posed in your environment. Risks should then be prioritised by criticality and impact, and reviewed for mitigation, transfer, or acceptance. Building a risk register to identify, track, and manage risks on a regular basis is a great way to ensure you are on the forefront of identifying critical risks to the organisation. Some categories of risk to consider in developing your risk register include: strategic, reputational, operational, transactional, and compliance.

- Risk register
  - identify
  - track
  - manage risks

5.2.3 Business Continuity Management (BCM)

BCM is the holistic management process that characterises threats to your organisation along with the business impacts if those threats are realised. It also provides a framework for building resilience with the effective response strategies that protects an organisation's brand, reputation, and stakeholder interests. The BCM is comprised of the Business Impact Analysis (BIA), Disaster Recovery Plan (DRP), and Business Continuity Plan (BCP). The BIA, is a document that complements the Incidence Response Plan (IRP) and one of the most critical business continuity activities. The BIA is a process that is designed to gauge effects of interruption that are critical to business operations in the event of a cyber incident, system failures, or other predicaments.

5.3 Business Impact Analysis (BIA)

Developing a BIA is an intensive activity that requires gathering a significant amount of data when meeting with business units and IT teams to determine Recovery Time Objectives (RTO). The RTO is an estimate of the maximum amount of time a business function must recover its system, processes and resume normal operations. This leads to a second component of the BIA, which is to determine the cost impact of various critical business functions during an interruption. A prime example can be found within any sector of the manufacturing industry, where loss in manufacturing functions results in orders being backlogged, thus affecting revenues.

5.4 Disaster Recovery Plan (DRP)/Business Continuity Plan (BCP)

Another important document includes the DRP. The DRP is activated during an incident where teams are working to mitigate a breach and then bring systems back online. It tends to be a very technology-focused document, whereas the BIA is heavy on the business side of things. A risk assessment and BIA will help determine where and how to focus various resources in the middle of a recovery process. Lastly, there is the BCP, which takes a more comprehensive approach to incidents. This includes moving business-critical systems to a segregated environment while containment takes place. Keep in mind, you're also attempting to continue performing business in the midst of a security incident.

5.5 Incident Management

Incident management is both a proactive and reactive process. It involves having proactive measures, such as strong detection capabilities so that teams may react appropriately when the response plan is activated. Incident management should also be closely associated with your organisations security awareness and training programmes. This ensures that all staff are trained and security incidents are minimised or do not happen at all. The first priority in incident management is to address life safety issues and then gather information that can be used to assess the incident, notify and escalate, triage, contain the incident, analyse the nature and source of the incident, track and document the incident and restore to normal operations. Not all incidents require the same level of reaction and do not necessitate the activation of the response plan. it is therefore critical to have to find severity or classification levels for different types of incidents, with the most severe requiring activation of your plan. There are various national and international standards for categorising incidents from organisations like ISO and NIST. However, your categorisation of incidents should reflect your business environment and your internal processes.

1. Address life safety issues
2. Assess the incident
3. Notify and escalate
4. Triage
5. Contain the incident (Stop it from spreading)
6. analyse the nature and source of the incident
7. Track and document the incident
8. Restore to normal operations.

5.6 Security Sources

Breaches can be detected by a wide range of security tools and sources, particularly those with automation detection capabilities. Though it can be challenging in determining the scope and severity. Ensuring you have a documented baseline of your environment can help your team distinguish between unusual but expected behaviour against something that could be malicious. Some resources and tools to consider in analysing a potential breach include

- **Log management**: This process revolves around generating, transmitting, analysing, and storing log data from systems. An important consideration here is the verbosity of logs being collected. Set logging levels from various systems to certify that critical pieces of information are not being left out.
- **Security Information and Event Management (SIEM)**: Reviewing logs and triggered alerts to get an overview of a potential breach. Typically, logs pulled into the SIEM are parts and will provide information such as source and destination IPs, hashes, traffic patterns, and data from packets to paint a high level picture of the events occurring.
- **Vendors**: Partnering with a managed security service provider has its benefits, as they're able to provide around the clock assistance with analysis of security events.
- **Threat intelligence (TI)**: Subscribing to threat intelligence feeds is a great way to expedite your teams response to a breach. Many TI feeds are industry specific, so you'll have access to other organisations, large and small, sharing their intelligence and offering guidance on solutions where possible.

5.7 CSIRP Activation

If a breach is confirmed, CSIRP activation is warranted and the lead incident handler from the security team is assigned. The lead is responsible for the following initial activities. Determine a central, secure documentation repository to collect all information pertaining to the breach. Delegate current and any new activities as they pertain to systems of interest. And determine when to initiate chain of custody actions for affected systems. The lead will oversee, administer and lead all operations involved in the incident handling process, including response, analysis, triage and reporting. This also includes functions such as crisis communication, forensic investigations and recovery procedures.

5.8 Scope/Impact

A breach is one of the most significant events that can happen to an organisation. Emotions can be high, the stress can be unmeasurable, and the financial and reputation impacts can be felt by all in the organisation. Although the headlines tend to focus on the financial impacts, the impacts of morale, productivity, and brand reputation can have a lingering effect that lasts for years. Direct and indirect financial implications aside, it is paramount to be able to quickly ascertain the scope and impacts of a breach. This is a crucial point in the response process, as actions will need to be prioritised based on the scope and impact of the breach. You will want to identify all affected systems, devices, data, and their classification. Review the preliminary details with the relevant IT teams to assist with the investigation efforts, determine the scope, and the potential impact of the breach.

5.9 Classification

When it comes to classifying a breach, you should be aware that not all loss of information represents compromise of data. Before you declare and classify a data breach, you should conduct a thorough analysis on the type of data that is effected, as well as the circumstances surrounding it. Be sure to also consider legal definitions and compliance requirements such as US Health Insurance Portability and Accountability Act of 1996 (HIPAA), General Data Protection Regulation (GDPR), and others, to determine when to declare a breach and the appropriate classification. The severity of a security breach should be documented in some fashion as well, those typically seen in the form of a matrix.

5.10 Breach Impact Analysis

The impacts of a breach can be felt almost immediately but it is important to consider the direct, indirect and systemic costs of a breach. Outside of the cost per record lost, there are impacts that affect the following.

- **Business lost**
  - This is a result of a loss of customers in a declining customer confidence.
  - Loss in employee productivity and turnover due to business system downtime, reallocation of staff to the breach response and those that leave due to the attack.
- **Brand recognition**
  - Breaches have a direct impact on brand value and often result in a drop in share value and an impact on the business' future opportunities.
- **Systemic cost**
  - According to the Ponemon Institute's 2018 Cost of a Data Breach Study, the average cost of a data breach currently sits at $3.8 million and the average cost of its lost or stolen record is $148. This doesn't include credit monitoring if payment card data was lost or back charges for those whose data may have been fraudulently used. it is important to consider the ongoing maintenance cost of dealing with a data breach. You can begin to realise just how costly a data breach can become on a company of any size in the short and long term.

5.11 Communication - Internal/External

During any high severity security incident, such as a breach, interruption to business processes are likely to occur. Triage, recovery, and restoring all operations to normal condition is the primary goal. At the same time, communicating with the right stakeholders, and providing updates on current activities in a timely manner, is equally as important. At this phase of the response process, you'll have an idea of the type of breach, scale and severity. Internally, you'll want to notify the relevant IT teams, affected business units, and the appropriate level of management. Building a communications escalation document, or matrix, can help drive decisions on when to communicate to different levels of management. Externally, there are a variety of options. If you're partnered with the managed security services provider, or security operations center, you may look to notify them so they can continue to monitor, and analyse the situation.

Caribou Coffee Hit with Security Breach at 265 Stores

5.12 War Room

The war room is where all the action happens and is an essential tool in incident response. it is a dedicated room where all CSIRT members gather in the event of a major incident. However, because the CSIRT must be in constant communication with other internal and external parties, it is imperative that appropriate communication

methods are in place. Often, normal communication channels may not be trusted when dealing with a breach and alternate methods for communication and collaboration must be considered in advance. Ensure there is a secure internet connection and bridge line restricted to those who need to be involved.

5.13 Chain of Custody

During this phase you'll also want to establish a chain of custody as you begin to gather and document evidence of a breach. The purpose of this is to serve as a paper trail for electronic evidence. It should specify the data collected, sequence of control, transfer, and analysis along with the name of each person who handled the evidence with the appropriate timestamps any time evidence is collected or transferred. This is imperative to ensure the integrity and authenticity of the evidence and prevent contamination which is paramount if it is needed in court.

5.14 Roles and Responsibility

When in the war room with members of your CSIRT, you'll want to establish a decision making structure and begin assigning roles and responsibilities to ensure adequate coverage of response activities. Roles and responsibilities should be laid out in your CSIRT, so everyone responding knows what is expected of them, as it is a time and cost-sensitive event. Depending on the size of your organisation, you may have each one of these teams with their respective responsibilities or multiple roles could be the responsibility of one team. Here are some of the technical teams involved.

- **Incident Response and Management team**
  - They're responsible for overseeing, administering and leading all operations involved in various incident handling activities, including response, analysis, triage and reporting.
- **Forensics and Investigation team**
  - They oversee the investigation process of the breach. Activities here include determining the root cause of any incident and collecting relevant snapshots and logs.
  - This team will work with any external security providers to receive additional logs or artefacts.
- **Recovery team**
  - They oversee and implement recovery strategies. This includes restoring servers to known good configurations, applying backups of network devices, patching affected systems, and general security hardening.

Although the core of the team dealing with response initially will be highly technical, you must understand that it is an organisational issue and not just a technical one. You'll be relying on non-technical teams to make sure your response is a success.

5.15 Team Coordination

One topic that should go without saying is the importance of coordination between members of the response teams. Even the best laid plans during a crisis have a tendency to go sideways. There's plenty of room for error, particularly if it involves coordination of a large team in conjunction with vendors and third-parties. During a breach, time is not luxury and there a lot of moving pieces that come into play quickly. The first 72 hours are critical and the actions and decisions you make during this window will have everlasting effects. The elite incident handler acts as a composer of sorts, orchestrating the activities and messages that get delivered to key personnel. Therefore, it is important to practice and plan for every impediment that might present itself. Everything must operate to the proper tenor so that all teams are working cohesively and not duplicating or impeding the work of another team.

5.16 Documents/Secure Channel

Documentation is instrumental when it comes to breaches or any other type of security incident. A secure document repository should be created internally with access limited to those involved in breach response activities. In this phase of response, you'll want to record and store notes from the initial detection events as well as analysis reports and more for reference. This allows you to stay focused on specific events, other team members to reference, review, or continue your work and for reproduction of the event by internal teams or third party responders. One particularly important document that should be created is a timeline of events. This helps teams remain organised, provide context at each event, and provide a total picture of the incident.

5.17 Building the Breach Response Plan

5.17.1 Methodology

Your methodology should define, from a high level, your organisation's incident response process, regardless of the scope and depth of your response. Your methodology will vary, but should include an overall flow and order of operations, in order to achieve a response that is effective, timely and repeatable. A CSIRP should outline the phases of your response methodology, including your organisation's pre-incidence activities, through to your activities performed after the incident has been closed and business operations are back to normal. Basically, you want to outline the high level activities that include your core elements of detection, declaration, investigation, containment, recovery, and post-incident details. Your plan will differ and have varying levels of granularity. But remember, the devil's in the details. The next section is all about your incident response and declaration. So, one thing to keep in mind, is that in the next few portions of this plan exercise, we're going to exercise a little bit of creative license. We are going to cover concepts that should be covered in this section of a plan, but you may have different headings or titles for the information. But regardless, the information should be included in your plan. Remember, your plan is unique and it should be catered to your organisation and your organisation's culture. In this section of your plan, you should outline your organisation's processes

for incident management. You should include some sort of severity index that ranks your incidents and at what level do you activate your CSIRP. Not all incidents will require the nuclear option. And in your day to day operations, you're likely dealing with hundreds or thousands of events. Therefore, it is important that you outline an incident severity index and what type of incident results in the activation of your plan. These processes may be outlined in existing documents and you should reference those here. You will state how your organisation defines and qualifies incidents, and at what level do you activate your plan. Remember, that once the plan has been activated, you set into motion a flurry of activities. And it is important to make sure your response processes reflect that. This is also an excellent place to outline any critical, first responder steps. Always remember the human component of your response. And first responders should be expected to memorise all the steps they need to perform during that initial phase of an investigation. So, it is imperative to document these activities and make sure that they are always kept current. It may also be helpful to link out to any standard operating procedures and checklists that you may have to reduce the chance of mistakes.

5.17.2 Initial reporting and distribution

The right message at the right time to the right people. Use this section to state the proper channels, messages and distributions of information. More often than not, you need to practice discretion when dealing with a breach. As you may come into contact with sensitive information, from interviews or from your initial investigation. This plan section should identify groups and messages. Templates are worth their weight in gold during the chaos, as it helps you to stay organised and takes the guess work out of your actions. Just remember not to leave any information out or to embellish, only report on the facts. There are many case studies on organisational breach, and many of those that reported incorrect information, suffered a severe backlash.

5.17.3 Facilities and technology

The key to proper response is, without a doubt, in planning. You will make assumptions and there will be some guess work as you do not have all the details yet. In order to make your life easier, and that of your team, it is vital for people to know they have a place to be to perform their activities. Your plan should include the members and locations for the teams to connect, collaborate, and manage the incident. Many organisations establish a war room for this very purpose. The war room also assists you when you need to perform activities with discretion. Having a separate meeting space to triage these activities will go a long way in controlling the stress everyone is feeling. Another key factor, that is often overlooked, is that of a zero trust environment. In a breach, it is likely that you do not understand the full scope, and normal communication channels and technology may not be trusted. You should plan for this and provide information on proper communication channels, how to access trusted networks, and the availability of backup equipment.

5.17.4 Breach procedures and documentation

For confidentiality reasons, it is wise to outline special incident management guidelines that should be used during an investigation. This is to limit the amount of detail, captured within your tracking system, or in some cases, may require the use of a separate incident management system in order to track tickets, as some investigations may involve internal employees that have access to those systems. Another concern is to outline protocols for sending encrypted communications. Again, we are working in a zero trust environment, and you want to limit the exposure of your many activities.

5.17.5 Contact information

Your organisation may already keep call trees and a master list of staff's contact details. You'll want to link that data here, or develop it separately, as you may want more contact points for emergency contact reasons that you do not want in your master contact list. This will vary for you, and you may choose to separate contact details by the phase of your plan. Or you may want them all in an appendix. However you decide to do it in your plan, you will want all the contact information in a singular location, and include several additional contact points, such as backup numbers and contact methods. There's nothing more frustrating than not being able to get in touch with key members during a crisis.

6 Immersive Exercise (Part 4) – Getting to grips with incident

The initial call has concluded and the various teams are starting to work on gathering more information. The good news so far was the detection procedures have worked. At least the systems did what they were supposed to. Reports are coming in and the investigation deepens. It looks like several different accounts had similar behavioural patterns on the network.

- Could there have been a coordinated attack?
- Or might one bad actor have been trying to confuse the investigation by using multiple accounts?

Again, logs have been tampered with along the way, and the path that these accounts took is not entirely clear.

Then, a call from the Network Operations Centre (NOC) comes into the War Room secure line. In the War Room, the SOC lead, Tom, takes the call. Everyone is watching as his face turns tense. With one look, he silences the room. This is the reality of these kinds of situations. They are ever evolving and changing. As new information comes in, it can add to the confusion. Something we initially thought might be small now appears to be much larger in scope. You really hope the team can hold it together.

He announces to the room, "*This has just escalated. The NOC has confirmed the attack vector, this is a confirmed breach. We do not yet know if the attackers are still active on the systems and we are going to have to start shutting down access and locking down the networks.*"

Though an incredibly difficult situation, your team was well chosen and together you have weathered some tough situations. This one, however, might take the prize. With every new piece of information, the severity level is moving up.

You follow on. "*There are going to be some serious business impacts from these steps. We need to stay coordinated. I want to keep the secure line open, but I need to see that encryption status report right away.*"

7 Immersive Exercise (Part 5) – PR Director ups the Ante

7.1 Investigation, Containment, and Mitigation

With the continued impact of this breach expanding, and with the risk level extremely high, you begin to direct the shut down of systems that might have been compromised. As soon as they act on one system, the ongoing investigation reports come in, revealing that the access was wider than previously thought. The stakes are raised and tensions increase. People are starting to get scared. The implications of ex-filtrated data could endanger lives. Things are moving quickly and hard decisions are being made. The selected shutdowns have stopped the automation-assisted production lines and processing systems in the factory. Keys are not being made. Production has ground to a halt without notice to facilities, sales, or even management. The head of Public Relations, Tanya, comes in the war room. She is demanding answers. She says, "*I do not understand. We know we have had a breach, but we do not even know when it happened? How can that be? I need to get in front of this. We have regulated timelines to report out. I know you already know that, but we need to have a narrative that makes sense or the media will run with it. Can you help me get a solid answer on this list of questions?*"

7.1.1 Investigation Overview

When it comes to investigations, whether internal or outsourced, it is important that the investigation team has the appropriate technical skills and a thorough knowledge of the scientific method and investigative process. Collecting digital evidence properly is one way to demonstrate the admissibility of the evidence later. Depending on the circumstance, this may be performed internally, externally, or a combination of the two. Either approach is fine, as long as the evidence can be properly used in a legal proceeding. There are five steps in the investigative process that are essential during an investigation:

- Identification
- Preservation
- Collection
- Analysis
- Presentation.

7.1.2 Identification and Preservation

When it comes to investigations, whether internal or outsourced, it is important that the investigation team has the appropriate technical skills and a thorough knowledge of the scientific method and investigative process. Collecting digital evidence properly is one way to demonstrate the admissibility of the evidence later. Depending on the circumstance, this may be performed internally, externally, or a combination of the two. Either approach is fine, as long as the evidence can be properly used in a legal proceeding. There are five steps in the investigative process that are essential during an investigation: identification, preservation, collection, analysis, and presentation.

The first step is identification. The investigator's first step in evidence collection are critical. Their job is to collect as much of the data as possible, take notes of all that they find, and prepare initial reports of findings. The investigator will start to identify sources of information and activity that is to be investigated, and determine a root cause. During this step, the investigator also learns what types of digital data and electronic devices might be involved in the investigation. At this time, the investigator will start to plan the tools and techniques that they may use during subsequent steps. Next is preservation. During this step, the investigation team will take measures to isolate and secure potential digital evidence, and ensure that it is not tampered with or destroyed. If the underlying case is a criminal case, the investigation team may work with the appropriate law enforcement agency to secure the crime scene. If the underlying case is a civil case, or an investigation for a private organisation, then the investigator will work with the person who has the authority to approve the collection of digital evidence.

7.1.3 Collection

The third step is collection. When beginning to collect evidence, it is important to understand where to look, and how to properly collect information related to a breach. The investigation team must ensure that they have the legal authority to acquire and collect digital evidence. Evidence that is improperly collected is not usually admissible in court. This means that the evidence cannot be used to establish facts or prove an assertion. Collection mechanisms used during this step will vary depending on the types of devices that the investigator is collecting. The investigation team will also document how the devices, and any evidence, were collected. This documentation is the beginning of the chain of custody for any digital evidence that would be presented in a court proceeding. A chain of custody document shows who collected the evidence, and how that evidence has been analysed and controlled during a case.

7.1.4 Analysis

Fourth is analysis. During the analysis phase, the investigation team will begin to understand and draw a clearer picture of the breach. The investigation team will examine the digital data and electronic devices that they've collected for relevant evidence. In most instances, the investigator will make one or more duplicate images of any electronic digital media. The investigator will verify that the duplicate image is identical to the original media but using cryptographic hashes. One duplicate image is used as a working copy that the investigator will review for relevant evidence. A second copy may be used as a control, or back up copy, in case the first working copy is somehow corrupted. During this stage, the investigator will use auditable, repeatable procedures to examine the digital media and produce a report of files or data that might be relevant to the underlying investigation.

7.1.5 Presentation

And finally, presentation. During this step, the investigator will report on their findings. The investigator must be able to show that the investigative process was completed properly and followed the scientific method. The investigator also must be able to show that they properly used any forensic analysis tools or software. The reason for this is to help demonstrate that the evidence collected is admissible in a court proceeding. Keep in mind that while there are a wide variety of tools available for forensic activities, your organisation's security programme should clearly define what forensic actions can be performed. Given these tools may capture sensitive information, your programme should also detail safeguards for the information, including secure storage, encryption and access control.

7.2 e-Discovery Overview

If your legal team says, send me the data you found on this case, how would you do it? What would be your first reaction? Would you send them a bit stream image, a folder with files, a spreadsheet listing file names? All of these options fall into one of two different approaches to e-discovery:

- Forensic
- Non-forensic

Of course, some in the industry take a blended approach to reduce costs, as adding additional steps to a workflow is ultimately more expensive. Let's briefly discuss these two approaches.

7.2.1 Forensic

If you were to use a forensic approach to e-discovery, you would follow digital forensic best practices during the collection process. This would entail identifying and preserving evidence in a way that accounts for its order of volatility and avoids modifying the original evidence wherever possible. For example, if you were tasked with performing a forensic e-discovery on 100 computers scattered throughout an enterprise, then you would need to consider the following.

- **Volatile memory collection**: Do you need volatile memory? Is that important? It shouldn't be as simple as saying this is a case that involves data from the past three years so we won't need RAM. With today's technologies and the way e-discovery software processes data, you might entirely miss a data source in your investigation if you do not know what was running on the system.
- **Hard drive acquisition**: Use a write blocker or similar methodology that is an accordance with best practices for a hard drive acquisition. Instead of copying files from the hard drive, to preserve the metadata of file system or operating system as much as possible by using a process or methodology best suited to the situation. So using an enterprise remote imaging solution to selectively gather the files within your scope makes much more sense that physically pulling out each and every hard drive.

- **Metadata and file integrity preservation**: When using your Forensic eDiscovery process, you should be preserving metadata from both the file system and operating system. File systems like NTFS, have a plethora of information inside of them, including log files, dates, times, and records of file changes. Operating systems have registries, property list files (plists), and log files. You should also ensure that files have a checksum that is calculated when collecting data. That way you can later verify that the data has not changes. A common validation method that is acceptable for file integrity purposes, is message-digest five, or MD5. Choosing to use a larger checksum such as sha256 will require additional CPU time to calculate the checksum with little upside.

7.2.2 Non-Forensic

When producing information, you need to ask yourself what's important, the entire file, including it is metadata, or just the contents of the file? If it is just the contents of the file, and not the dates and times, then you have a lot of options when processing data. You can collect data using various techniques, including the built-in copy and paste features of many operating systems. You can also create remote network connections to logical folders, and collect data with a simple drag and drop. The key in this scenario is using a process that is acceptable and has built in checks and balances to ensure mistakes are not made. The steps for non-forensic e-discovery are designed to be procedural, but also account for scalability. Since cases can range from one custodian to thousands very quickly, it is often helpful to have a logical model of framework for these steps that can be followed. Here, reference the Electronic Discovery Reference Model (EDRM), as it is a standard that is not tied to any one specific vendor or company. This model has nine steps, and each of these steps has its own individual process and documented procedure. While this course does not delve deeply into each step, you can learn more by visiting the EDRM site.

Electronic Discovery Reference Model (EDRM)

7.3 Digital Evidence

Earlier, we briefly touched on establishing a chain of custody, which serves as a paper trail for chronological documentation of digital evidence. Sources of digital evidence stem from two categories:

- **Any device that has memory**: This category includes computers, tablets, and smartphones. Keep in mind that this category may also include networking equipment such as routers, switches, and wired or wireless devices. It also includes office equipment and storage devices.
- **Any service that transmits data or any provider that stores data**: This category includes email, websites and apps, cloud storage providers and ISPs. Regardless of its form, however, it is important to remember that evidence is generally fragile. Evidence loses its value if it is not collected, preserved, and protected in a proper and timely manner. Items and objects that lose their evidentiary value very quickly are called fragile. Digital evidence can be especially fragile. it is easily destroyed by a simple keystroke, sent across a network, and possibly changed or damaged by intervening physical forces such

as electromagnetic fields. There are two general types of digital evidence and each type has different fragility issues.

Persistent data is generally considered less fragile, because it is preserved on storage media, when an electronic device is powered down. Even though the data is preserved when a device is powered down, this type of data can still be tampered with and overwritten.

Volatile data on the other hand, is very fragile, and is held in the memory of a device, or in connection with another device. It can exist in cache, random-access memory, and registries, and is lost when devices are powered down. Cyber-forensics professionals must take special care in collecting and preserving this type of evidence, so that it remains valuable.

7.4 Tracking Evidence and Chain of Custody

A Chain of Custody form should be used any time evidence is recovered and transferred. This is the heart of the evidence tracking process. The first part includes:

- Lists the case number, offence, name and title of the person seizing the evidence, name of the victims, date, time, and location of where the evidence was seized.
- **Description of each item that was seized**: The row immediately underneath the last item described should contain the words FINAL ENTRY and a line should be drawn through the rest of the fields in that row. This prevents additional evidence items from being added to the form after the form is completed.
- **Details the actual Chain of Custody**: This part of the form should document each time the evidence was handled and each person that handled the evidence. This figure shows the third part of a typical Chain of Custody form. Notice the fourth entry on the form. This entry is a good example of how evidence is transferred from one agency to another while still maintaining the Chain of Custody. Evidence should only be transferred using a delivery service like FedEx or UPS that offers package tracking. Also, a signature should always be required when sending evidence to another agency.
- **Final disposition of the evidence**: The evidence is returned to its owner or destroyed if it contains something illegal or contraband that cannot be legally returned to the owner. All digital storage devices should be forensically wiped prior to being returned to the owners. By following these steps you'll be preserving the integrity of the evidence from alterations. Should evidence be found altered, it may be challenged and found inadmissible in a court.

7.5 Evidence Preservation

Preserving digital evidence starts with collecting it. The techniques and technology used, must be appropriately secure, and result in the preservation of evidence. In addition, all applicable rules and laws must be followed. Any deviation from these best practices, can be destructive to your case. Once evidence is collected, we must look to its preservation. First, it is a general rule that original evidence must remain pristine. That means no forensic work should be performed on it. Rather, an exact digital copy of the evidence must be made. For example, when we are preserving a disk, we generally make a bit for bit physical copy, otherwise known as a disk image.

7.6 Investigation artefacts

Bad actors often leave behind traces of their activities as they navigate a network and compromise a system. artefacts left on a system, network, or disk can provide insight into the attackers activities going back quite some time. Searching for these artefacts can help your team create a timeline of the attackers lateral movement and help determine a point of entry. Reviewing logs from a variety of sources including fire walls, routers, and intrusion and detection systems, will provide pieces to complete the puzzle.

7.7 Case Management

Case management is a means of collecting, distributing, and analysing information about any type of IT incident. From a security standpoint, however, it serves as a compendium of information, analytics, and collaboration about the breach. it is also important to create a secured document depository. Custom workflows can be used to build out a flow of automated activities in relation to the incident.

7.8 Third Party Involvement

Depending on the size of your organisation and type of business they're involved in, it may be difficult to staff a dedicated incident response team. This is fairly common, as one or two teams may take on multiple roles and responsibilities. As such, most organisations identify the roles they feel their internal staff can satisfy and then look towards a third-party responder that can have the necessary skills, experience and know-how that will support them in their time of need. While third parties may be experts in their respective fields, they will still need to be working with your internal teams and be managed efficiently in order to maximise response efforts. Provide all third parties involved with context on the situation, direction as to what they can and should be assisting with, along with expectations for the work to be completed.

7.9 Tools

Some tools you may use when conducting investigative and forensics activities include firewalls. These are network based devices that inspect network traffic and allow or deny it, based on configured rules. Firewalls can be configured to log as much or little information about traffic allowed and denied as you want. Some even have packet capture capabilities to an extent. Information logged here generally includes time and date stamps, source and destination IP addresses, and the port number and protocol utilised. If your firewall is configured for Network Address Translation (NAT), you may have additional data around network traffic that can be reviewed.

- **Intrusion Detection Systems (IDS)** There are two types of IDS's: network-based and host-based.
  - **Network-based IDS**: use sensors to monitor for network traffic, but can't necessarily see the activity happening on a host itself.
  - **Host-based IDS**: would be required, and installed on individual work stations and servers to monitor for a nominalist activity.

  Both types of IDS tools can be signature-based or anomaly-based.

- **Honeypots**: Honeypots are machines set up on the network that are intentionally insecure. This is designed to draw attention to potential attackers to attack the honeypot system, instead of a real one. Honeypots do not contain any sensitive information, but provide insight into malicious activity on your network.

- **Packet sniffing and capture**: Packet sniffing and capture tools are a common way to examine traffic on specific portions of your network. The sniffer will require access to a network adapter that works in promiscuous mode, and a driver to capture that data. Once captured, you will be able to apply filters to review the details of specific packets related to a security incident. This will greatly assist in developing your incident timeline.

7.10 Containment

Containment is all about limiting the damage to your environment, data, and cutting of points of entry for the attacker. A strong containment strategy will afford the other members of the incident response team time to develop a remediation strategy. However, the scope of the breach plays a role in how you contain it. Based on the information gathered during your detection and analysis cycle, as well as the evidence gathered during your investigation, you'll want to paint a picture of just what the scope is and identify all compromised hosts. Attempting to contain a breach without this information can leave you exposed. Take measures to contain and control the breach to prevent further unauthorised access to or use of personal information on individuals or corporate data. This includes shutting down specific applications or third-party connections, reconfiguring firewalls, changing computer access codes, and modifying

physical access controls. Here are some of the common but effective strategies to isolate effected hosts and prevent the situation from escalating. Remove the attacker's ability to access the environment and the attack record that was used to gain access. Firewall, DNS, and web-filtering blocks are instrumental here. Close off the initial attack vector and any similar ones. Do not access or alter the compromised system. Disable potentially compromised user or service accounts. Do not turn off the compromised machines. Instead, isolate the systems from your network. If it is on a wireless network, change the wireless network pre-shared key on the access point as feasible and remove the other authorised devices that maybe using the corporate wireless network. Naturally, making decisions quickly and accurately is critical at this stage. You will be more successful if your organisation has predetermined and well documented processes and approaches for containing various types of incidents.

7.11 Mitigation Strategies

Mitigation is where you'll begin to address the root cause. Like the containment stage, you'll want to have a mitigation strategy that fits your environment and organisation. Some common mitigation strategies include:

- Changing all applicable passwords for IDs that have access to personal information, including system processes and authorised users.
- If it is determined that an authorised user's account was compromised and used by the intruder, disable the account.
- Running antivirus scans across your network to verify no payloads have been dropped as a result of the breach.
- Delete any malware you find.
- Revoke and issue new certificates where possible.
- Fail over to a backup instance.

Mitigation should be carried out in a phased approach, as there are inter-system dependencies to take into consideration.

7.12 Cross team Communication

Cross-team communication is a crucial component of every phase. Performing accurate analysis and sharing that information to other members of the Cybersecurity Emergency Response (CSER) will insure that everyone is on the same page. In responding to a breach, time is of the essence. Communications will reduce confusion and keep people aware and oriented. Teams that should be in constant communication include the :

- Security team
- Incident response team
- Network team
- Forensics team.

This article reviews the importance of timely communication:

Making a bad situation worse: how Equifax mishandled the breach

7.13 Building the Breach Response Plan

- Building the Breach Response Plan document
  - NIST Special Publication 800-86

- **Investigations**: Start with the investigation components ahead of other actions, as not to impact your evidence collection. A little bit of a disclaimer. Like with the first section, this section only intends to cover the components of an investigation in the context of a breach. If your organisation intends to consider litigation or you're expecting to have to answer a e-discovery request, you'll want to consult with an expert as you will want to avoid spoilation of your evidence. Without ensuring the proper steps are followed, evidence could be lost in a manner similar to inadvertently wiping off fingerprints from physical evidence. The investigation process is about finding answers and transitioning from detection to containment. This involves discovering the source of the problem, understanding when it happened, how it happened, which areas of the business are affected, and with which methods you should use to respond. Once the incident is contained, the remediation and recovery process can begin. An organisation's response to a data breach speaks volumes. Depending on the severity, it'll be analysed and scrutinised by many different parties, including regulators, lawyers, management, customers, and other stakeholders. They will not only want to know how and why the breach occurred, but also the steps that were taken to gather evidence, to determine the scope. Did we secure compromised systems? And have we notified those that were affected? This section of your plan should outline your methodology and process associated with investigation efforts. Special care and considerations, and perhaps working with experts, will help you outline the specifics in regard to collecting forensically sound evidence. Third-party involvement should be outlined in this section, such as working with outside digital forensics firm. Unfortunately, we can't cover every component that should be included in this section of the document, as it'll vary from organisation to organisation, and the sample text provided only demonstrates a small portion of the components that should exist in this section of your plan. So consider all of your organisation's processes, and start to outline those components that make sense to your organisation, and just fill it in as you go and start connecting the dots. A great resources for building investigations into your incident response is NIST Special Publication 800-86, which is the Guide to Integrating Forensic Techniques into Incident Response.

- **Evidence Gathering and Handling**: Handling electronic evidence requires extreme care. Unlike the traditional evidence we associate with a crime scene, like blood splatter, footprints, and shell casings, electronic evidence is fragile. A failure to properly mark, secure, and protect such evidence could result in accidental data corruption or the complete destruction of all the data. Different types of electronic evidence require different methods of marking, securing, and protection. This section of your plan should very clearly state your policies and process around investigations, such as evidence gathering, your evidence lifecycle, any processes you have around chain of custody, your templated chain

of custody forms, e-discovery procedures, and your how-tos on how to perform an investigation against your different assets. You'll perform a different type of investigation for your cloud systems, mobile devices, physical workstations, or your virtual machines. Evidence management is also critical to the success of its use in court, and equally critical to its use in a non-legal environment, such as in an incident response within your organisation. The bottom line for all evidence management is make sure you have the appropriate SOPs. Follow them rigorously. Document thoroughly. Always maintain the chain of custody and securely store the evidence.

- **Response and Business Continuity**: No one said that leading an incident was an easy task. Not by any means. At this stage, the teams and the incident lead are very carefully juggling multiple work streams, and this is why planning and practising is vitally important to your incident response. Investigation activities must be handled carefully, and your initial response activities should support the ongoing investigation, but also recover the organisation back to being fully functional. organisations should ensure that incident response policies and procedures are connected to your business continuity processes. They must be in sync. Cyber incidents undermine business resiliency. Proper recovery does not happen until the threat has been contained and mitigated, but connections need to be made that identify where your breach response activities and your business continuity or disaster recovery plans intersect. At this point, business continuity and recovery staff should be made aware of the incident and its impact so they can start to begin reviewing the business impacts, new risk, and the continuity of operation plans. Tight coordination, detailed instructions, and having the recovery team on the ready can allow for certain tasks to run in parallel and minimise the operational disruption.

- **Containment**: Containment activities are important, as they prevent the threat from continuing to spread throughout your organisation. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making, i.e., making decisions around shutting down the system, disconnecting the network, or disabling certain application or system functions. Such decisions are much easier to make if they are prearranged strategies and procedures for containing different incident types. organisations should define their acceptable risk when dealing with incidents and develop their strategies accordingly. Containment strategies will vary based on incident type. For example, the strategy for containing a malware infection is going to be quite different than that of a network-based attack. organisations should create separate containment strategies for each major incident type that they have, with criteria documented clearly to facilitate the decision-making process. Also note, the failure to contain could result in increased liability. If the attacker uses your systems to attack another, a delayed containment strategy is therefore dangerous because it may allow the attacker to compromise other systems. Another consideration regarding containment is that some attacks may cause additional damage in your attempt to contain it, such as logic bombs or

encrypting data upon removal, so have contingency plans in place for dealing with these types of incidents.

- **Mitigation**: Or some people call it eradication. So after an incident has been contained, mitigation will be necessary to eliminate the components of that threat, such as deleting the malicious software, or disabling user accounts, as well as identifying and mitigating the vulnerabilities that were exploited. You'll want to identify all the affected hosts so that they can be remediated. For some incidents, mitigations may not be necessary, or maybe they'll be completed during your recovery phase, but once a resource is successfully attacked, it is very often attacked again, or other resources within the organisation are attacked in a similar manner. Mitigation and recovery processes should be done in a phased approach so that the steps are prioritised, defined, and reduces rework. For large-scale incidents, recovery may take a long time. The intent of the early phases should be to increase the overall security relatively quickly to prevent those future incidents. Later in the recovery phase, or even in the post-incident phase, you should focus on those longer-term changes, those core infrastructure changes, and the ongoing work to keep the enterprise as secure as possible.

- **External Entities and Communications**: As your breach response advances, so does the sphere of influence and involvement. This may include communications in coordination with internal and external entities. This could include your external Sarbanes-Oxley (SOX), a forensics firm, outside legal counsel, business partners, law enforcement, your Internet Service Providers (ISP), your software vendors, and other organisations and other entities that will be unique to your organisation. It is paramount to keep a mind-map of sorts of all the internal and external teams you'll be working with during this phase. This portion of your plan should then map the processes and all the templates for communicating with each of these various parties.

7.14 Self Test

1. Which of the following is NOT a step in the investigative process?
   - Presentation
   - Detection
   - Identification
   - Preservation
   - Collection
   - Analysis

   Answer: Detection

2. It is acceptable to perform forensic work on original copies of evidence.

   Answer: It is not acceptable.

3. Non-Forensic e-Discovery is designed to be procedural but also account for scalability, since cases can range from one custodian to thousands very quickly.

   Answer: True

4. What is NOT the right course of action in containing a breach?
   - Close off the initial attack vector
   - Turn off the affected hosts
   - Isolate the affected hosts from the network
   - Implement firewall, DNS, and web filtering blocks

   Answer: Turn off the affected hosts

8 Immersive Exercise (Part 6) – Plant Director raises the stakes

8.1 Recovery and Notification

The team is trying to divide and conquer, and some have started working on the answers to the PR-related questions. You do not think that is the best use of time, but you can't micromanage each step, so you keep your head down and continue managing the containment. If the team doesn't stay focused, you are going to have to intervene soon.

The Plant Manager, Richard, comes into the War Room. He says, "*What do you mean I won't be able to run the factory systems for the next four hours? That will cost an incredible amount of money. Are we supposed to just have 35 line workers stand around and wait? You have to be able to get those systems back up immediately*."

You know there is no way to do that right now without opening yourselves up to continuous vulnerabilities, so you try to explain that to the Plant Manager. He does not like what he is hearing, and is pushing you for alternatives. It is starting to feel like chaos.

The tension is growing between the team members. Blame is being traded. One team member accuses another, "*What do you mean you reran the logs from the SIEM? I just queued that job too. We can't be wasting time doing the same work. You need to communicate.*"

The accused replies assertively, "*That is not helpful. You know that the SIEM logs are in my domain of expertise and it makes sense that I would doing it. We should all be doing whatever we do best at this point.*"

8.2 Recovery

Recovery is where affected systems are brought online and back into the production environment carefully. To ensure it would not lead to another incident. This is unlike the containment stage, where the focus is preventing a fire from spreading. The type of recovery not only depends on the time and financial needs at your disposal, but also on the amount of damage caused by the breach to your environment. Take note that once the system has been attacked, there's a decent change it will be targeted again as the attacker attempts to utilise the same attack factor as before. Some key decisions to take into consideration during recovery include what patches and other remediations should be applied, time and date to restore operations. IT and business system owners must coordinate to make an appropriate decision on when the system should come back online based on the advice of the CSIRT. Test and verify that the compromised systems are clean and fully functional. Ensure backups for affected systems are clean. Ensure monitoring is in place to observe for abnormal behaviours. It is imperative to document all decisions made during this phase, including what tools are being used to test, monitor, and verify the compromised systems are not vulnerable to the same attack methods.

8.3 Recovering Environment

During a breach, you may find your number one priority is to bring back the organisation to an operating state. During this phase, you should have a better understanding of the method of attack and affected systems. However, it is vitally important that when you begin to recover systems that you do not make too many assumptions and not take anything for granted. Trust but verify. Regaining control. At this point in your response, you're trying to get the affected systems back to a known, good state. You may have isolated systems and services during the investigation phase. You want to make sure that your recovery efforts do not impact any evidence or contaminate the crime scene. Additionally, you do not want to restore a system that is still susceptible to the same attack. There are steps that can be taken to decrease the likelihood of a repeated compromise. These steps can include: system hardening, the process of securing a system by reducing its vulnerability and attack surface. Deploy additional monitoring, adding additional layers of defence such as a firewall or adding an IDS or IPS to the system. Changing systems, application and user credentials, you would not be able to trust any of the accounts on the machine and you should change passwords for all access types for the system. Controlling backups, you do not want your backup system to be contaminated or to recover the wrong version or instance of a system. So controlling who and how people can recover infected machines should be highly controlled. Use indicators of compromise, you should look for artefacts on the machine that might indicate a known exploit or attack was used. Tools and checklists can go a long way to help to determine if there are any indicators of compromise still on the system. Certifying the environment. All systems should be certified and validated before placing them back into production. it is vital to have a process in place that certifies the recovered systems and provides you with high confidence that the breach was properly scoped, no evidence exists of additional breach or ongoing intrusion, and that you are able to better prevent, detect, and respond to future attacks.

8.4 Recovery Considerations

- **Complexity**: Complex systems are the thorn in the back of good security practices, and dealing with complex services and applications during response can slow things down. Therefore, when recovering, it is important to think of the service in its entirety. Your application could consist of multiple load balanced and distributed front ends that connect to an assay service database and have integrations with multiple third-parties and services. The more complex the system, the more likely recovery could be delayed. Therefore, it is important to document and test regularly using scenario based incident response.

- **Business services**: Similarly, the collection of systems should be viewed in terms of business services it supports. Technology teams during the recovery phase are likely to be focused on the system that it services. In the flurry to get things back to our normal operating state, they may overlook or skip verifying that all the proper business functions are working.

- **Order of Operation**: The order in which you bring systems up could have an impact on its functionality. This may seem like a no-brainer, but any number of things could go wrong when engaged with breach response. This is why testing your plan and conducting tabletop exercises using various scenarios will prepare you for the real deal.

- **Value of documentation**: There is nothing more reassuring during an incident than to have excellent documentation to rely on. It takes a lot of the guess work out of recovery. Clear and easy to follow documentation can speed up recovery time and increase confidence in your recovery measures.

- **Change management**: Due to the fluid nature of breach response, and with the flurry of activity, standard operating processes and your governing structure for change, may present a hindrance. Therefore, it is necessary to outline in your CSIRP your process for dealing with emergency changes to systems and configurations.

- **Communications**: As with all phases of breach response, your messaging needs to be clear, concise, and delivered to the right audience. Developing communication groups in advanced will make sure you are delivering the right message to the right people, at the right time.

8.5 Recovery Strategies

- **Recover data**: Business Impact Analysis (BIA) critical in the event of a breach.
- Business Continuity Plan (BCP)
- Incident Response Plan (IRP)
- **Maximum Tolerable Downtime (MTD)**: is the time after which the process being unavailable creates irreversible consequences generally, exceeding the MTD results with severe damage to the viability of the business. Set by business senior management.

8.5.1 Maximum Tolerable Downtime

The following are common MTD estimates organisations may use. This will vary from organisation to organisation, and between business units as well.

- **Non essential**: 30 days
- **Normal**: seven days
- **Important**: 72 hours
- **Urgent**: 24 hours
- **Critical**: minutes to hours.

8.5.2 Recovery time objective (RTO)

The RTO assumes there is a period of acceptable downtime in the event of an outage. This is an estimate of the maximum amount of time a system can be

unavailable before it is outage begins to affect other systems, business processes and the MTD. Recovery point objective, also known as the RPO. This is the acceptable amount of data loss measured in terms of time. It represents the earliest point in time at which data must be recovered. The greater the value of the data, the more resources can be put in place to ensure minimal losses in the event of a breach or other disaster. Work recovery time, also known as WRT. This is the remainder of the overall MTD value, and deals with data recovery, testing processes and finally getting everything into a business normal and operational state in production.

Collectively, these measures define the level of acceptable risk for a given organisation in the event of recovery. Other helpful data collected that should be part of your plan include resource requirements. In order to restore business operations, what resources might be required? Facilities and workspace equipment, data, personnel, and supply chain. However, special care must be taken when performing your organisation's recovery procedures in the context of a breach, as trust has been lost for these information systems. All of this information enables the organisation to decide on recovery options. The plan for how to recover business to an acceptable level within the acceptable time frame. The speed of recovery necessary to meet the RTO and the data continuity necessary to ensure critical functions will dictate which approaches the organisation will utilise in recovery operations. The following sections detail some of the techniques and methods for supporting recovery efforts.

8.6 Active defence

8.6.1 Introduction

As you begin the process of recovering systems into their normal production state, you'll want to implement additional security controls for monitoring purposes. As stated previously, there's a chance the attacker may attempt to breach the same systems again and you want to keep an eye out for anomalous behaviour. While you want to implement tools for this, addressing things from risk management perspective is just as important. NIST's information systems continuous monitoring framework breaks this concept down into three tiers for an organisation wide view.

- Tier 1 - Organisation (Governance)
- Tier 2 - Mission/Business process (Information and Information flows)
- Tier 3 - Information System (Environment of Operation)

Tier one, this tier addresses the organisation as a whole and its drivers are governance, risk management goals, along with the risk appetite and tolerance for the organisation. The tolerance levels are defined by executive leadership. Tier two, this focuses on mission and business processes. Criteria for continuous monitoring at this level are defined by how core business processes are prioritised with value to the goals and objectives of the organisation and the security programme. Tier three, this tier addresses monitoring from an information systems standpoint. Some activities here include certifying that all technical, operational, and management controls are implemented appropriately, operate as expected and yield the outcomes that meet security requirements.

The article reviews how important proactive monitoring can be to preventing a breach.

eBay Breach Highlights the Value of Monitoring Security-Related Events

8.6.2 Automation

Automation is the key component at this point as it can make the process more efficient and reliable in monitoring for anomalies. Automated tools can identify patterns that may escape the human eye particularly when analysing great volumes of logs and data. Some suggestions for automation include:

- Setting a baseline level of logging and auditing
- Creating a log retention policy that specifies how long log data should be contained for business critical systems.
- Ingest log sources from affected business systems and build rules and alerts for anomalous behaviours.
- Monitor sensitive directories for unusual activity like mass copying or deleting of files.
- Create a schedule to conduct vulnerability scans on a regular basis. Then track and remediate those vulnerabilities based on severity.

A sample timeframe for scanning based on levels of data sensitivity are:

- **Low level**: every 180 days
- **Medium**: every 90 days
- **High**: every 30 days
- **Critical**: every three days.

Schedule antivirus scans to run on a frequent and consistent basis. Work with a third party security provider to conduct internal and external penetration tests alternating every year. Build a remediation plan to address issues that have been discovered. This should also be documented in the risk register.

8.6.3 Wrap Up

The right balance of adding additional controls, hardening, and building a cyber-defensible position after recovering from a breach can be difficult to achieve. There are many pitfalls organisations can fall victim to during their response. These pitfalls, including adding unnecessary tools and controls, and focusing on the root cause and not the big picture. The best advice to improving your cyber-resiliency post-breach is to go back to the basics. Review the data you are trying to protect, and create a balance between your organisational needs, value of the asset you're protecting, your risk environment, and the unique threats your organisation may face.

8.7 Notification

8.7.1 Introduction

Communication acts as your lifeblood and anchor, during breach response. There will be an ongoing communication between internal teams and external stakeholders. it is critical to have a consistent process for communication, throughout your CSIRP, that outlines the appropriate audiences, the type of message, and when the communications should happen. The CSIRP should account for all affected audiences, such as, but not limited to: employees, customers, vendors, investors, business partners, advisory groups, law enforcement, and regulators. Your plan could also include templates and guidelines, for the various messages. Messaging will be affected by your legal and regulatory environment, and any jurisdictional considerations. do not make ambiguous or confusing statements about the breach. it is important to stick to the facts. do not withhold key details that might help consumers protect themselves and their information. Also, do not publicly share any information that might put consumers at further risk.

8.7.2 Internal

Internal communications. During the notification process, you'll want to notify a wide range of audiences about the current situation. Business units affected by the breach should be updated on recovery plans and timelines. organisation executives and board members should be kept in the loop as well, particularly if the breach involved any kind of data loss. Internally, your business team should be aware at least at a high level that a breach occurred and has been remediated. Since many employees likely work with customers daily, they should be trained to a system and should have the right messaging and talking points on hand. Internal employees should be trained on how to deal with media inquiries and other concerns that are likely to be flooded with.

8.7.3 External

External communications. Externally, you'll want to work with your legal and PR team in communicating the breach to a few different groups. Customers affected by the breach should be informed of the date of currents, data affected, and recovery efforts. Regulators are a key group you should report to, particularly if you have to meet compliance requirements, such as Payment Card Industry (PCI) and HIPAA. The European Union has its own set of regulations to comply with in the event of a personal data breach.

Beyond regulations, you may have local laws to follow in reporting data breaches. The media will certainly get wind of an incident at some point, and you'll want to work with your legal and PR teams to craft an appropriate response to the public. They are the go-to points of contact for any media inquiries, and you'll want to assist your employees to redirect any questions from external sources to them.

This article reviews how an initial poor response can still be managed to a good conclusion: Target credit card hack: What you need to know

8.8 Building the Breach Response Plan

- **Recovery Environment and Strategy**: You should describe or even illustrate your recovery methodologies and approaches. This section of your plan should contain all the details necessary to ensure that the recovery phase can be performed in a consistent and repeatable manner. Including your plan references to your disaster recovery or your business continuity plans, or alternatively, you can define those in this section of your plan. Fundamentally, how you restore your environment will depend on your business continuity that you have in place. A BC or DR plan is something that you should have set well in advance to create fail-safes of sorts so that you have contingency plans for any loss of services from a breach or any other event, such as weather, fire, or other natural disaster. Business impact assessments inform these plans. If you have not performed a proper or recent BIA, your recovery objectives may be obsolete and are no longer in line with business objectives. BIAs should be performed annually, at a minimum, and the results should influence your DR and BCP priorities. Recovery environment and strategy. So in this section of your plan, you should provide all business continuity management materials that may be needed or referenced in order to facilitate proper decision making, such as any documents related to crisis management, continuity of operations and disaster recovery, and scenario details that you might have. This portion of your plan should also include any scenarios that you've developed, decision trees and work flows. This phase should also include those steps that will assist in mitigation and posturing. For example, you should include processes for rotating credentials, keys and secrets. Your incident response team must work with system owners to ensure any system-to-system communication is restored and remains in working order. Effective response management extends beyond preparing for any specific type of event. Your BCM should include the development of broad, flexible capabilities that enable response to a wide range of events along with their various magnitudes. Your CISRP response strategy should define how you lead, prioritise and communicate during your recovery response. organisations should align response strategy with the organisation's culture, responsibilities and values. A sound strategy frames a cost-effective, well-sourced organisation-wide approach to addressing recovery from cyber incidents. A well-developed strategy will minimise tunnel vision in response and reduce the adverse impact to operations and revenue.

- **Certifying and validating**: After an incident, critical business operations must resume as soon as possible. This is in order to minimise disruptions that generate financial, reputational, regulatory and even stakeholder impacts. Remediation begins after critical business operations resume with short-term and long-term efforts to close the gaps. The organisation must verify that the attack vectors are eradicated and that steps have been taken to prevent similar attacks in the future. Remediation must eliminate or minimise root causes of incidents and return business's functions, IT and stakeholders back to a secure operating environment. You want to have trust in your restored systems. In this portion of your plan, you should outline the resources that the response teams will use to

test, validate and certify systems. This part of your plan should outline the activities that will ensure that your systems are not only back and operational, but are no longer prone to attack, including the people, processes and technology that will be used for this purpose.

- **Breach notification**: NIS, NIS2, GDPR. I'm sure those terms probably elicit some very strange emotions inside of you, and every organisation will have different rules, laws and legal and regulatory obligations, depending on their location, vertical, and their national or international laws. So use this portion of your plan to identify your organisation's specific breach notification requirements and develop key messages and templates as well as processes that identify the proper personnel that will be responsible for these notifications and which groups they'll be reporting to.

9 Immersive Exercise (Part 7) – Getting to grips with the Chaos

You announce, "*Okay, enough is enough. We have a CSIRP for a reason. We need to get back to the plan. You quickly see nodding heads and see some of the tension dissipate"*.

You continue, "*This is a stressful enough situation without adding team squabbling to the mix. I know everyone is tired and frustrated, but we've got to remain on track and on the plan. Roles are assigned based on the plan. We made those decisions when we developed the plan for a reason. We have no time to waste. Let us go around the table and identify the responsibilities from the plan. You will be contacting the appropriate stakeholders. You will be managing containment and chain of custody. You will relay with PR and communications to ensure we have met regulations and are giving the right information at the right time. You, could you please make more coffee? Thank you.*"

9.1 Self Test

1. What are some things to consider before recovering systems affected by a breach?
   - Complexity
   - Business Services
   - Order of Operation
   - All of the above

   Answer: All of the above

2. Active defence is the concept of implementing additional security controls for monitoring purposes, especially on systems and resources that were affected by the breach.

   Answer: True

3. Automation is a key component of which tier?

   Answer: Tier 3

4. When communicating to external parties, which groups of people should be notified of the breach? (select all that apply)
   - The media
   - Regulators
   - Customers
   - Government and law enforcement

   Answer: All of the above

10 Immersive Exercise (Part 8) – Recovery and Notification

10.1 Post-Incident Review

Progress slowly begins to be made. Everyone is reminded of their roles and things are becoming clearer. The investigation is wrapping up and the next steps for communications are clear. You've now progressed into the Recovery and Notification phase. Systems need to come back up and you need to get production up and running ASAP. You have the data you need. You just need to be sure you protect it. The plan is working. The team has remembered what they put into it and why. The right information is coming in from the right people and they are making the best use of their time. The shutdown has locked out the bad actors for now and the data is captured to build a case. The team has a plan for the post mortem and will be able to complete an after-action review in an orderly fashion. Systems are being restored and production has resumed. All appropriate parties are in tight communication with their respective response liaison and everyone is on point and on message with those requesting information. Meanwhile, the Forensics Team will continue their investigation and work to develop and document strategic recommendations for future enhancements.

10.2 Reporting

We've reached the final phase of the Incident-Response Lifecycle, your systems are all back online, and functioning as intended. You've removed the tact factors and artefacts left by the attacker, what next? The first thing to do is to put together a post incident report, which should contain several sections.

- **Incident identification information**: Note the date and time of discovery and its notification, the incident duration, and the reporter name and contact information.
- **Executive summary**: A high level overview of your findings that includes enough information for someone to understand what you did.
- **Incident root cause**: Here, you select the root cause of the incident along with the severity. Note down the description of the incident itself not the actions you've taken. After that, you'll want to identify all the systems impacted by their host name and IP where applicable. - want to **Chronology of events**: to include communications, discoveries, etc. This is where all the information documented earlier comes in handy. From there, summarise the actions the team took to remediate and recover from the incident.
- **Items reviewed**: This section lists and memorialises everything you are relying on to draw your conclusions and opinions. Typical items to be listed in this section include, but are not limited to, deposition, transcripts, digital evidence items, and the oppositions expert report.
- **Acquisition methodology**: Describe the process in which you acquired evidence. You should be comprehensive in detailing your process and methodology. Keeping in mind that you are satisfying both industry best

practices, and the legal requirements to admit evidence to trial. It is typical to see some form of data validation listed in this section. For example, MD5 values for the evidence collected.

- **Analysis**: This section can vary based on the scope of your analysis, but you should describe what tools and techniques you used as well as your results. If you used multiple tools, you should provide tool version numbers so your results can be cross validated by another examiner. This section should provide enough information so that another examiner who is provided your evidence files, should be able to confirm or dispute your findings.
- **Conclusions**: This section should clearly indicated what your conclusions are based on your analysis. To be successful at trial, you will need to provide supporting evidence to support your findings.
- **Evaluation**: This serves as a lesson learned type of session and it is all about learning and improving.
- **Sign off**: The report should be signed off by your organisations Chief Information Security Officer (CISO) or Chief Information Officer (CIO), and stored in the secure repository. Once this is complete, you'll want to get the team together to review the report, especially the evaluation section. Improvements can always be made somewhere along the line and it is imperative that your team incorporates those changes as soon as possible, be it policy, or procedure.

10.3 After Action Review

After action review, there can be positive outcomes that come from a breach response. One in particular is that there are no better ways to test your plan and finding out shortcomings than to practice it in real time. There is an opportunity to learn from the real thing and improve your organisation's ability to detect, respond, and prevent future breaches. The learning your teams will experience during an actual breach incident will carry with them throughout their career. The after action report allows the response teams to share with stakeholders what went well and what didn't.

10.4 Post Mortem

Post-mortem, holding post-mortem meetings allows for those involved to reflect on the experience, and share their input that will improve future responses. It also helps in the development of next steps, and additional action items that need to be completed. One key to running these meetings, is to avoid blame, and keep the meeting focused on improvement, and not punishment for what went wrong. Post-mortems should review each phase of the life cycle, and not focus on one area specifically.

10.4.1 Public Post Mortems

organisations have also been known to share post-mortems with the public so they can gain an understanding of what happened. Although most companies may shy away from releasing too many details to the public, it can allow you to have a reasonable and defensible cyber position to use for future litigation that may arise from the breach. An example of a post-mortem shared by an organisation is the report produced by the GAO, or Government Accountability Office, for the Equifax breach.

This is the GAO Post Mortem for the Equifax Breach:

DATA PROTECTION: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach

10.5 Building a Comprehensive Timeline

Building a comprehensive timeline. A detailed timeline of the breach and all of its associated activities has multiple benefits. it is an asset that can tell the whole story of what transpired at a quick glance. It can assist in determining the resources used and where there may be deficiencies. For example, once all your items are on a timeline, you may determine that the root cause conclusion was not reached in a reasonable amount of time or that promised service level agreements were not met and work hard to availability of a business service. One of the unfortunate outcomes of a breach is that of litigation. Having a detailed timeline will help your defence in showing that you showed your due diligence in your response efforts. Whether in the courtroom, or dealing with regulators, a detailed timeline can help demonstrate succinctly what transpired and how you responded. The organiser will be challenged to defend the actions taken during a breach and your record of events will make clear what happened.

10.6 Law Enforcement

If you've reached to law enforcement at any point during the breach, be sure to provide them with the evidence found during your investigation. Ensure the chain of custody is still followed and monitored for preservation of evidence integrity. Your organisation may decide to pursue legal options if the culprit is found, in which case you'll want to provide them with all documentation, relevant log sources, and more from your analysis as well.

10.7 Strategy and Assessment

Following a breach, there will be without a doubt a flurry of activity. Your business teams and council will be hard at work doing damage control, protecting the brand, and image of the organisation, and preparing for litigation. From the perspective of the information security professional, you can expect a lot of questions, and a razor sharp focus on the efficiency of the security programme. The security team will likely be the persons who provide the debrief to stakeholders. But once that's completed, expect a heightened awareness around the governance of the programme. The key is to stay ahead of this activity, and use this as a way to improve your programme. There are steps you can take to show ownership and accountability, by performing tasks such as rebaseline against a standard.

- **Adopt or rebaseline your programme against the cybersecurity framework** want to Measure your organisation maturity against that standard. There are many popular frameworks, such as ISO 27001, NIST CSF, PCI DSS, or CIS Critical Security Controls. Many of these standards have corresponding toolkits that can make the task of standard adoption easier, and provide you with strategies for it is implementation.

- **Maturity models** want to Many of the standards also have maturity model assessments, that can help an organisation quickly identify where they are on the maturity continuum. Understanding where your organisation fits into these models will allow you to complete an analysis, which will provide a comparison of your security programme against best practices. By comparing these best practices to your organisations actual practices, you can shed light on areas where vulnerabilities and risks are lurking. The maturity models also assist in developing plans to move from your current state to your desired target state.
- **Gap assessment** want to Upon closure of an incident, a good next step would be to conduct a security assessment against your policies, processes, and procedures, to better understand your organisation's overall security posture, and ultimately tie back to the concept of people, process, and technology. This can be done internally, but bringing a third party with a fresh set of eyes can make a big difference. The assessment should cover your entire security programme, and identify gaps and areas of improvement. Because security assessments are risk-based, the results should be documented in your risk-register for tracking and mitigation. Keep in mind, that an assessment is different from an audit, as it focuses on how strong or weak your posture is, as opposed to measuring against an industry standard.
- **Forward thinking and business value** want to The importance of forward thinking following a breach cannot be stressed enough. The response team will be judged on how the breach was handled, and also by the changes and improvements to be made, so that it doesn't happen again. Developing a plan and sticking to it will ultimately result in the response teams' success. Developing a culture of security, and being able to sell the value it brings to the organisation, can sway an attitude of security from being an insurance-type activity, to being a business enabler, and gaining a competitive advantage.
- **Ramping up your offensive security**
  - **Penetration testing** want to Penetration tests are a very effective way to quickly find major issues in your environment, and it is recommended that you have one conducted by a third party, after experiencing a major breach or incident. it is also important to rotate the vendors who perform your tests, as some firms have different areas of expertise. Ensure that you create a Scope of Work (SoW) document, detailing exactly what kind of testing will be done, what systems will be tested, hours of testing, and whether the testers are allowed to test any exploits discovered. This document should be very thorough, as you want to avoid any 'oops' moments. Especially since it is a production environment. A report will be generated at the end, and you'll receive suggestions on how to mediate discovered issues.
  - **Red Team and Blue Team exercises** want to Another consideration to make is that, practice makes perfect, and by having technical staff participate in attack simulations can increase the skillset, and familiarise them with the concepts and processes of breach response. These types of exercises are commonly referred to as Red Team and Blue Team exercises. These simulations have you divide your staff into an attack, red, and defence, blue, team. These exercises are designed to identify vulnerabilities and find

security holes in an organisation's infrastructure. This war games of sorts can also be used to test technical staff on your CSIRP and IRP.

- **Responsible disclosure and bug bounties** want to Another way to find and mitigate vulnerabilities, that could lead to future breaches, is to employ a responsible disclosure and bug bounty programme. This type of programme allows security testers and researchers a way to responsibly disclose potential threats to your organisation. These programmes can be managed internally, or by partnering with one of many providers that rewards testers for reporting bugs. This is important as it allows you to identify issues and mitigate them, preventing widespread misuse by a malicious actor. The benefits of a responsible disclosure and bug bounty programme, are that you will have a greater number of people with diverse skill sets looking at your organisation security. Also, the types of testing and vulnerability checks are typically more diverse and sophisticated. Testers participating in a bug bounty are incentivised to find bugs through a result-reward oriented model. Organisations that incorporate a paid bounty programme will likely see the cost of running the programme, far outweigh the costs associated with a breach.

This article reviews a well-regarded response to a breach:

This Company Was the Latest to Suffer a Data Breach. Its Reaction Was Perfect

10.8 Outreach and Public Relations

Outreach and public relations. When a data breach is made public, the impact to an organisation's reputation can be damaging and lasting. Customers' trust could be lost, thus impacting financials. it is important to be transparent and honest and avoid delaying communications or updates. Ensure your legal and PR teams have a strategy to tackle this to prevent your brand from being tarnished. Once the crisis of the breach is past, your organisation will need to do some rebranding and a media relations strategy goes a long way in that.

This article reviews questionable practices in notification and remediation:

Uber paid hackers a $100,000 cyber bribe to destroy stolen data

10.9 Internal Training

Now, we land at people, specifically employees. After you've gone through a breach, you'll want to build a user education and training programme, or bring in a third party to do so. Providing hands-on exercises to employees will give them a better understanding of spotting security issues, and learning to report them. Building on your security culture is paramount, and a continuous effort that shouldn't stop. Offering training twice a year is a best practice, and performing regular fishing campaigns is a great way to educate.

10.10 Cyber Insurance

As you've learned, risk management plays an important role in cyber security. And this is just as true with breaches. Cyber insurance is a way of reducing risks associated with breaches. Cyber insurance does not completely mitigate liabilities but it can help in reducing them. Cyber insurance is designed to help organisations reduce or mitigate risk exposures by offsetting the cost of recovering from a cyber security breach or other incident. According to Price Waterhouse Coopers (PWC), one third of US companies have some form of cyber insurance. And given the frequency of large scale breaches, this may be a wise investment for your organisation. Some things to consider when shopping for cyber insurance include, does the policy cover any type of attack your organisation falls victim to? If not, which specific ones are covered? Does the insurance assist with response activities like recovering compromised data and repairing damaged systems? How are coverages and limits applied?

10.11 Plan, Do, Check, Act (P-D-C-A) Cycle

Lastly, upon the closure of a breach, you may look to make drastic changes to your environment as a means of continuous improvement be it data flow or new tools. Regardless, the Plan, Do, Check, Act method can be applied to plan for improvement by showcasing your plan as one of continuous improvement. The breakdown of the PCDA cycle is as follows:

- **Plan**: Before making changes note down what problem you're trying to solve or activity you want to improve and how you'll calculate the effects of the change. This can be anything from number of incidents because of a specific problem to the time spent on configuration, cost savings, and more.
- **Do**: Once your goals have been outlined, make the intended change.
- **Check**: After implementing the change, you should test, validate, and begin to track metrics to measure it is effectiveness. Improvement is expected, however sometimes there may not be a change or it actually worsens. For instance, creating additional training material for your employees on top of what's provided may end up being too difficult or cumbersome to grasp.
- **Act**: This step largely depends on the results of Check. If the change was a success, and you're seeing the expected measurement of effectiveness, you should begin to update the relevant people, documents, and perhaps other technologies to reflect it. utilising this method can help create a culture of continuous improvement especially if you tie it back to risk.

10.12 Practice Practice Practice

Finally, the key to an excellent response plan, particularly after suffering a breach is to practice, practice, practice. Running training programmes, table top exercises, breach scenarios and playbook exercises will dramatically improve your next response. Processes should be repeatable and easy to follow and staff should be immersed in the plan regularly so that their roles and responsibilities are clear. Then, when the rubber meets the road, you can have confidence that the plan will be executed quickly, responsibly and with precision.

10.13 Building the Breach Response Plan

- **Reporting**: This plan section will include all the pertinent information that must be included in reporting out your final synopsis of the incident, to include the who, what, where, when, and how the incident. Reporting groups will be defined in this section, as well as your various templates, reports, and different audiences. A summary of the incident with associated collaterals, such as timeline, summaries, and activities, should be provided to the business shortly after the bulk of your response activities. The document should be sent to these groups in a way that prevents unauthorised distribution. These should be delivered in a way that protects confidentiality and integrity of the document. it is also a good idea to send this report with right management functionality enabled. That way it requires proper authentication before anyone can review the report. You do not want this information getting into the wrong hands. As you may now realise, the response to data breaches, it includes a lot of moving parts, and having standard templates that allow quick and clear summary and communication, especially during the first couple of hectic days is absolutely critical. Having a team of reporting specialists who are familiar with those templates and who can quickly grasp what's important to track and what noise to filter out can be a life saver, after action and postmortem. Despite a flawless execution of your plan, the activities contained within it, unfortunately do not end. Following a breach or any major incident, you should outline all the post-incident activities to include any after action reports, postmortems, meetings, committees, and improvement plans that will be expected from you post-incident. So do not leave out this last step. Take this opportunity to learn from your experience by improving and standardising your response process. So that your organisation is better prepared for the future. Hold a "lessons learned" meeting within one week of the close of the incident to ensure everyone's activities and thoughts are fresh in their minds, and make sure everyone checks their feelings at the door. All team members, especially leaders, they have to be comfortable talking about the errors and successes that happened during the breach response. The focus of the meeting should be on performance and metrics. Be open about constructive criticism, while examining every phase of the operation. The result of this meeting should be a list of identified probable causes, identifiable errors. That way you know what could be done differently to improve the result next time.

- **Legal and Law Enforcement**: So we've talked about legal implications pretty much throughout the plan, but we call it out here at the end, specifically, because it is vitally important to identify those processes and procedures on how you will handle the legal and regulatory implications of the breach. So there's the legal components while in the middle of the response. And then there are all the legal implications that happen after. So in this portion of your plan, you want to identify the collection of laws that may apply to you and the protections provided by the jurisdiction of any of your data owners or customers. You will have consulted with legal throughout, but in the context of post-breach, your plan should outline how you intend to work with your legal counsel, for either expected litigation or if legal prosecution is pursued by your organisation. You should define your strategy for dealing with law enforcement. These sections of your document, they can be sensitive and will vary widely depending on your country, your jurisdiction, where you are. You'll want to work with your legal counsel, and make sure there are clear organisational processes and consensus on how you will preform these activities.
- **The incident response team should become familiar with your various law enforcement representatives**: before an incident occurs to discuss the conditions under which incidences should be reported to them, how the reporting should be preformed, and what evidence should be collected and how it should be collected.
- **Training and Practice**: Practice makes perfect, and the only way that you're going to succeed in the middle of a crisis is to have practised your plan several times in advance of an actual incident. In this section, you should outline your tabletop exercises, test scenarios. Determine who will be responsible for the testing and maintenance of the plan and how often you'll be providing training to staff and to the actual CSIRP members. Your tabletop exercises, you talk about how they'll be facilitated, how the workshops will be ran. it is usually a good idea to do discussion-based exercises, where staff can meet to discuss the roles, responsibilities, and coordination and decision-making of a given scenario.
- **Strategy and assessment**: Have a plan and strategy of how you'll deal with the flurry of activities that will happen post-incident. Having a pre-prescribed set of events already defined will help your organisation be able to move forward with confidence in the improvement plan, the processes and people behind the response plan, and just generally feel confident in the security of the organisation and your path forward. In this section, you want to include your processes and plans for gap assessment, working with penetration testing companies, third-party audits, and how you're going to go about improving your security posture. These activities and plans will help you be prepared for when someone inevitably asks, "What's next?" or "Are we secure?" or "What have we done so this doesn't happen again?" So that's it folks. I've had a pleasure going over the components of the plan with you. And I hope that you've learned something in these segments that you can take back and improve your plan. So that way that you are prepared for the worst case scenario.

10.14 Self Test

1. What are some things to consider before recovering systems affected by a breach?
   - Complexity
   - Business Services
   - Order of Operation
   - All of the above

   Answer: All of the above

2. Gap assessments conducted after remediating a breach are a good way to review and identify holes in your security posture. What concept does this apply to? (Select all that apply):
   - People, Process, and Technology
   - Risk Assessments
   - Business Continuity Management
   - Security Awareness and Training

   Answer: All of the above

3. What can be done to minimise the impact to an organisation's reputation after a breach?
   - do not inform the media, customers, or public about the breach
   - Ensure your legal and PR teams have a strategy to prevent your brand tarnishing
   - Be transparent and honest, and avoid delaying any updates to relevant parties
   - Rebrand the organisation entirely so it appears like a new company

   Answer:
   - Ensure your legal and PR teams have a strategy to prevent your brand tarnishing
   - Be transparent and honest, and avoid delaying any updates to relevant parties

4. What is the purpose of cyber insurance?
   - Help organisations reduce or mitigate risk exposures by offsetting the costs of recovering from a security breach or incident
   - To help purchase security tools
   - Provide security services in the event of a security breach or incident
   - To stop hackers

   Answer: Help organisations reduce or mitigate risk exposures by offsetting the costs of recovering from a security breach or incident