F-Secure

BLUE TEAM

BUILDING RESILIENCE THROUGH RESPONSE PROCESS DEVELOPMENT AND SIMULATION

ISSUE 2
An F-Secure Consulting whitepaper

THE F-SECURE GUIDE TO RAINBOW TEAMING

F-SECURE CONSULTING

F-Secure Consulting is a research-led cyber security consultancy, partnering with enterprises and early adopters worldwide. We exist to build resilience in an ever-changing digital world by providing evidence-based security advice. Our research drives service innovation, pushing the industry forward.

We're a multi-disciplinary team, equally intellectually curious and passionate about security. It's this that compels us to solve the world's most complex security challenges.

www.f-secure.com/consulting
Twitter: @FSecure_Consult
Linkedin: showcase/f-secure-consulting

CONTENTS

Driven by industry advancement in recent years, there is now a broader range of initiatives available to support the development of an organization's cyber security posture across the Predict, Prevent, Detect, and Respond (PPDR) model. Combined, these are colloquially referred to as a "Rainbow Team", delivering purple (collaborative), blue (defensive), red (offensive), and gold (crisis management) activities. When delivered sequentially and continuously, organizations gain the ability to utilize outputs from each development area and measure incremental improvement.

Each paper in this four-part series explores one such testing approach through the eyes of the teams – external and internal – leading and participating in the engagement. The aim: to demonstrate how the practical and technical delivery processes lead to real-world impact. For readers who have taken part in similar testing activities already, the series will help explain how to boost the benefits of that pre-existing investment.

The sequencing of rainbow teaming activities depends on the security testing and implementation your organization has carried out, and the experience of your security staff and senior security stakeholders.

THIS PAPER:

UNDERSTAND THE NETWORK, AND BUILD CYBER RESILIENCE BY IMPLEMENTING KEY DETECTION AND RESPONSE MEASURES.

BACKGROUND

Despite organizations seeing increased budgets, the 2019 Verizon Data Breach Investigations Report reveals nearly 40% of data breaches will take months to discover – and years for around 20%[1]. Users, systems, and data can be contaminated or lost altogether during this period, but the window of time – and the potential damage – can be reduced by putting defenses in place using detection and response measures. When an attack occurs, defensive security is a means to ensure your organization is prepared and able to act quickly.

The term "blue team" is used to refer to both internal and external roles that function in this defensive capacity. Also known as the Cyber Security Incident Response Team (CSIRT), it is commonly comprised of the Chief Information Security Officer (CISO), Threat Intel (TI), the Security Operations Center (SOC), and Incident Response (IR) team.

Whilst many organizations have an internal SOC, the IR team role is usually filled by an external partner. Maintaining an in-house IR team is an expensive proposition. Significant overheads and reduced levels of incident-handling skills (due to infrequent real-world experience) increase the challenge of keeping pace with the modern threat landscape. Skills atrophy and limited time or resource to keep up with modern threat actors, due to a narrower aperture of modern threats, are two examples of this knowledge gap. As such, outsourcing IR usually makes sense for organizations from a financial and practical perspective. Still, during an incident, internal stakeholders retain responsibility for decision making and relevant escalations regardless of where the IR function sits. This requires the right people, processes, and technology positioned to effectively respond to a certain level of threat.

To measure and improve the effectiveness of a blue team strategy, the tools at its disposal, and the methods it uses in response to threats, defensive testing, also known as "blue teaming", is needed.

Blue team engagements can be broadly broken down in to five areas:

- Technical Detection Uplift
- Technical Defensive Training
- Response Process Development & Simulation
- Incident Response Engagements
- Strategic Defensive Consultancy

The focus of this paper is Response Process Development & Simulation. For this type of engagement, F-Secure works to assess an organization's readiness and capability to respond to an incident. This is performed in order to help them develop improvements and provide recommendations to improve that capability.

[1] https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf

WALKTHROUGH

The following walkthrough depicts a Response Process Development & Simulation engagement. For the purposes of this paper, we'll use a fictional client, Acme Bank. And to provide a true-to-life demonstration, we will base the walkthrough on the recent real-world engagements of our own Incident Response team.

PHASE 0: SCOPING

F-Secure Consulting is approached by Acme Bank. The organization comes having already conducted collaborative testing, including purple team activity. This was run in the aftermath of a real breach. Having now made alterations based on the findings of the exercise, key stakeholders are keen to conduct a blue team engagement to further test their IR readiness and resilience against attacks of all levels.

The engagement begins with a scoping discussion between members of F-Secure's IR team, and senior client-side security staff. Acme Bank is a large financial enterprise, with a global presence, and over 30,000 employees. This includes a dedicated security team and 24/7 SOC. Despite a mature security posture, continual fast growth has hindered the organization's ability to upskill staff and deliver strategic improvements to the resources and instruction at hand.

The SOC has documented ample low-level procedures, but no guide outlining the course of action when under attack.

As such, it is decided F-Secure will fill this deficit by helping Acme Bank in the development of its playbooks. To further test the SOC's understanding of these, and their ability to follow their guidance within the confines of their existing security tooling, workflows, and technical skill level, the engagement will conclude with a simulation exercise.

The playbooks will be delivered as flow diagrams that guide best practice incident response processes within the organization's SOC. Playbooks form part of the preparation phase of the IR lifecycle[2], but their content often spans other phases, including the post-incident review phase.

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

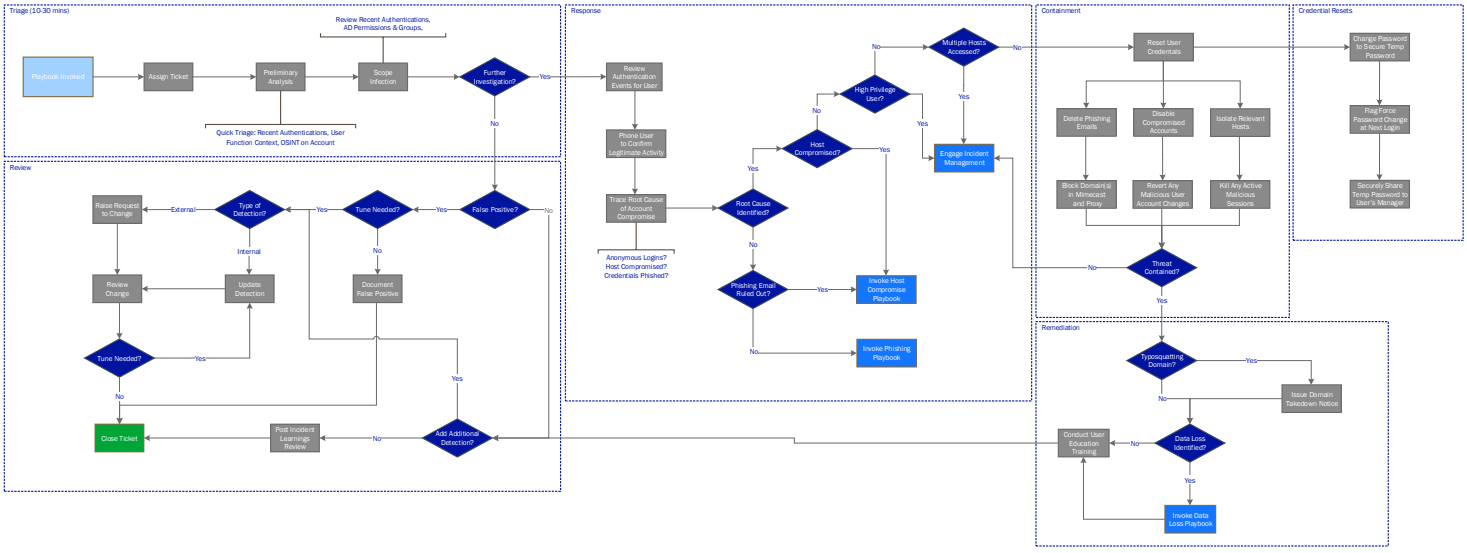

Fig. 1. Example playbook

PHASE 1: DISCOVERY & ASSESSMENT

Facilitators from F-Secure conduct interviews with key stakeholders to begin the engagement and develop their knowledge of Acme Bank's security limitations and strengths. The interviews focus on key stakeholders, including the CISO, SOC Manager, and Incident or Problem Managers. Questions are designed to help F-Secure understand how Acme Bank's security would resolve incidents currently, as well as gauging the flow of information in its decision-making process. They will also spend time with the SOC analysts on duty to examine their standard workflow and understanding of internal processes. Interview questions center around:

- Policy
- The response plan and strategy
- Communication
- Documentation
- The team
- Access control
- Tooling
- Training

The facilitators then review existing IR process documentation to calculate how IR would work for Acme Bank now, in the event of a real incident. These documents include incident management processes and SOC processes. The CISO is asked to flag others of relevance.

The interviews confirm the CISO's initial assessment that despite the maturity of its internal function for IR, it is underdeveloped for cyber security incidents specifically. This conclusion is familiar to the facilitators, who have both worked with similarly sized enterprises.

Despite ample procedures, there is no overarching framework for dealing with higher-risk incidents that require an orchestrated response. This is highlighted further through accounts of how past major incidents were handled. Although security and IT staff have proficiency within specific processes, their capability lacks planning and development. It also transpires there is confusion regarding the prioritization of IR processes, and a vague understanding of the organization's critical assets – an appreciation of which is fundamental in the design of a defensive function.

By the end of the discovery & assessment phase, the facilitator has enough knowledge to develop playbooks that will directly integrate with Acme Bank's existing IR process, whilst also improving the effectiveness of its security incident management. They share a top-level report detailing their findings.

Areas of strength:

- Dedicated security function with a 24/7 SOC and well-trained analysts
- Strong low-level procedures documented
- Mature general IT incident management function
- Good suite of detection and response tooling

Areas of weakness:

- Internal technical stakeholders lack experience managing large scale incidents
- Lack of "security" considerations in organization's incident management processes
- Little awareness of organization's critical assets
- Roles and responsibilities not clearly defined for stakeholders in case of a large scale incident

Before the engagement is contractually agreed, a clear set of objectives is defined via discussions between the security team at Acme Bank and F-Secure's IR team. The format and scope of playbooks is agreed, having understood the potential threats to the organization, and the availability of relevant stakeholders ratified. The facilitator is keen to emphasize the collaborative nature of a successful exercise, drawing attention to their dependency on the organization to engage openly throughout.

The high-level topic of the simulation scenario is also agreed to ensure it matches the organization's requirements: an advanced threat actor has gained domain administrator (DA) access to their core corporate domain and is attempting to laterally move to more critical systems.

Engagement objectives and commercials are confirmed in addition to a plan for the engagement, detailing when and where relevant stakeholders should be available.

PHASE 2: RESPONSE PROCESS DEVELOPMENT

Phase two of the engagement represents the largest portion of scoped time, as the playbook facilitator begins developing the new playbooks. Playbooks can cover many areas, including:

- Account Compromise
- Data Loss
- Denial of Service
- Host Compromise
- Major Incident Management
- Phishing
- Ransomware

With no playbooks in place currently, the facilitator advises Acme Bank to start with their top two highest priority topics. Trying to cover too many topics in a single engagement will ultimately lead to poor results. Based on existing threats, the areas chosen are Major Incident Management and Account Compromise. Once the simulation phase has helped establish the format, structure, and assumptions in the two new playbooks are compatible and value-adding, the rest can be developed as part of a long-term collaborative project.

A master playbook will also be included to form a foundation for all investigations. All playbooks are developed collaboratively with the organization, through an agile workflow that engages relevant stakeholders for feedback throughout the process. Each encompasses detection, triage, investigation & response, containment, remediation, and post-incident review sections. This involves direct involvement from the SOC manager and a stakeholder from the incident management team.

The process of playbook development is as follows:

- Review the bank's IR plan and processes in more detail
- Create flowcharts for each playbook topic
- Each flowchart is then broken up into the phases of IR
- Low-level procedures are created for the flowcharts to define each step, as well as assigning responsibility

It transpires through the review of its IR plan and processes, there are serious weaknesses in some of Acme Bank's incident scoring[3] practices. These are updated as part of the engagement to align with past security incidents and the guidance of the new playbooks. The updates ensure escalations can be made correctly, and incidents can be prioritized in direct relation to the tangible risk they pose.

There are also limitations to some of the bank's existing tooling that would hinder the investigation & response phase of the engagement. This tooling is under a proof of value (POV) phase, thus the feedback played a crucial role in the assessment of its suitability.

To conclude this phase, a session is held with all Acme Bank stakeholders present to review the new playbooks. F-Secure advises them on how to most effectively implement the playbooks internally, and a date is agreed for the blue team simulation to take place.

The simulation exercise is scheduled in a month and half's time, to enable the CSIRT to familiarize itself with the new playbooks, and develop strategies accordingly.

[3] https://www.us-cert.gov/CISA-Cyber-Incident-Scoring-System

PHASE 3: SIMULATION

Using the scenario agreed in Phase 0 as a starting point, the simulation sets out to test understanding and adoption of the new playbooks by analyzing the wider blue team's response in a simulated attack scenario. F-Secure will run a full day exercise with these technical stakeholders – the SOC manager, an analyst, internal incident management, the CISO, internal IR personnel, and the Data Protection Officer (DPO).

The scenario is a realistic reflection of the organization's risk profile as well as a good scenario to test a wide range of the content in the playbooks: an advanced threat actor has gained domain administrator (DA) access to their core corporate domain and is attempting to laterally move to more critical systems.

Whilst in some cases it makes good sense to involve executive stakeholders in a simulation, it often becomes detrimental to the learning of both groups. When running technical and non-technical content concurrently, participants may lose interest or struggle to contextualize the series of events when their roles are paused.

Alternatively, the exercise can be split into two parts, starting with a blue-team-specific version that runs up to the point of escalation to the executive level. The second phase is held with the executive team a week or two afterwards, using the outputs from the technical session as inputs in what is a specific Crisis Management Exercise (CME).

The blue team exercise taking place with Acme Bank is led by the second IR facilitator, who specializes in simulated scenarios. They will illustrate the scenario and provide direction throughout the day. As the exercises are designed to emulate as accurately as possible the series of events in a real-world incident, the facilitator will assume the mimicked position of external stakeholders, such as the press, Acme Bank customers, and relevant regulatory bodies.

During the exercise, the facilitator will closely monitor the team's actions and responses to events, to identify weaknesses that could potentially impede their effectiveness during a real incident. Examples of such include:

- Communication and coordination within the team and with stakeholders in other parts of the business
- Tasking and prioritization within the team, progress monitoring, and responsibility assignment
- Adherence to procedures set out in its incident response plans, as well as failure points in the practical implementation of these
- The team's acumen when dealing with technical investigations, and their knowledge on the systems and architecture in the organization

The facilitator will further aim to critically challenge any of the team's actions or decisions. This is to both test the team's reasoning and insight, and highlight decisions that, in their experience, could likely not be implemented practically during a real incident.

TIMELINE OF EVENTS

10:00

The bank's CSIRT convenes, following the discovery of a live attacker's presence. The team is briefed on the current state of the investigation and associated findings by the SOC representative. An initial risk assessment is performed according to the CSIRT's incident severity scoring procedure, and the results are communicated to relevant stakeholders outside the CSIRT. Responsibilities for specific workstreams are assigned to CSIRT members according to its incident response plan. The CSIRT breaks and will reconvene at the end of the day.

10:30

Feedback from the operational risk department suggests the risk posed by the incident is not fully understood outside of the CSIRT. This seems to be due to a misalignment between the CSIRT's severity assessment procedure and the organization's risk management framework. It is agreed a representative from operational risk will join the CSIRT for the duration of the incident to assist in this regard.

11:00

Analysts responsible for the investigation report they have discovered the attempted execution of a credential dumping tool on a domain controller. The associated account seems to be part of the domain administrators' (DA) group. The CSIRT is reconvened at short notice, and the incident's severity rating is upgraded to critical.

The representative from operational risk management advises since no evidence has yet been presented that the attacker is targeting any business-critical assets, other parts of the organization will likely not assign this issue the priority it deserves. A collaborative effort begins to contextualize the CSIRT's findings to clarify the potential impacts in business terms.

12:30

Investigators report that malicious actions involving at least two domain administrator accounts have been discovered on multiple domain controllers. They consequently advise the corporate domain should at this point be considered fully compromised.

The CSIRT's detailed playbook for containment of a full domain compromise is put into action. However, a representative from the domain architecture team advises deployment of the endpoint access management tool – which the containment procedure relies upon – has not been fully commissioned. This is due to it falling behind schedule since the playbook was created. A workstream is initialized to investigate alternative strategies.

The facilitator communicates the updated severity report sent earlier from the CSIRT has triggered an emergency Crisis Management Team (CMT) meeting. This meeting will happen in approximately 15 minutes, with the CSIRT expected to present a full situation report.

14:00

The investigation team reports they have discovered at least 2 external IP addresses used by the attacker for command and control (C2). Analysis of network logs shows 14 endpoints have made or attempted to make connections to either of these addresses in the last 24 hours. This includes the jumpbox providing administrator access to the isolated environment where the merchant payment processing service is hosted. When the CSIRT's incident response plan was created, the cyber security team was assigned the responsibility of maintaining a roster of system owners for all critical assets in the organization. A recent change in departmental ownership of merchant payment services was accurately captured in this roster, and the appropriate manager is immediately contacted. The CMT is informed of this development.

The IT team's system naming convention suggests 10 out of the 14 affected machines are user workstations. The CSIRT decides all workstations believed to be under the attacker's control should be removed from the network immediately. The exercise facilitator advises 3 of these fall under the management of the securities trading department, and the shutdown request has been refused by the associated manager; the downtime would be too costly and the CSIRT does not have the authority to order the shutdown. A review of the response plan shows the CSIRT indeed has the mandate to enforce such requests during a critical incident, although this has not yet been formally ratified by the organization's executive management team.

15:00

The investigation team reports an analysis of network logs has shown up to 200 endpoints across multiple regions may have been in contact with the attacker's external IP addresses over the last 7 days. While the team wishes to investigate some of these further, the organization does not currently have any tooling available that would enable large-scale remote forensic analysis – this capability was promised in the next version of their EDR tools. Manual artefact collection for endpoints hosted in the building is ongoing, but investigations into three servers hosted in another region are still delayed due to pending travel arrangements.

While the CSIRT does not have a playbook dealing specifically with an attacker moving between many systems, the incident management lead identifies the "Malware Outbreak" and "Ransomware" playbooks are flexible enough that they may be adapted to contain the current attack. Access limitation procedures defined therein are put into action, requiring collaboration between multiple technical departments.

The facilitator informs the team that the CSIRT has received a formal mandate from the CMT to proceed with disruptive containment actions, but with specific exclusions around client-facing systems.

15:10

Containment activities are underway, as per the new playbooks. The CSIRT is now under pressure to provide a time-to-recovery estimate to the CMT, and planning is started on this phase. The eradication and recovery strategy contained in the "Domain Compromise" playbook appears relevant for the situation. This calls for the involvement of the business continuity management (BCM) team.

A BCM representative reveals, however, they have not prepared procedures to implement the strategy outlined in the playbook. They further remark the CSIRT and BCM teams should ideally have collaborated in the process of creating the relevant eradication and recovery plans.

15:45

The containment, eradication, and recovery strategy is evaluated critically by all participants, and a consensus is reached it would likely be effective. Points where collaboration with other teams outside of the CSIRT would be required or helpful are identified and noted for follow-up discussions.

The facilitator informs participants the audit and accountability department has requested a full incident log that clearly shows a timeline where information became available, decisions were made, and actions were taken – along with the reasoning behind each. Despite a supporting member of the CSIRT having been given the responsibility of keeping such a record (as prescribed in the incident response plan), that person was not present in a number of meetings that happened outside of the CSIRT in which certain critical decisions were made.

Participants are interviewed to establish the facts while their memory on these is still fresh, and the results are added to the incident log as an annexure. The incident log is also preserved for the security team to use as a basis for improving their response plans to prevent the same mistakes from being made in future incidents.

16:00

The end-of-day debrief provides an overview of the outcomes that could most obviously be improved, as well as those demonstrating success. For Acme Bank, obvious challenges include the misalignment between the CSIRT's risk assessment framework and that of the wider organization, one of its playbooks' reliance on technology that has not yet been fully deployed, and a lack of visibility into the CSIRT's response plans from other teams that may need to be involved.

PHASE 4: REPORTING

At the engagement's final phase, the facilitators compile a report for the simulation exercise. This is supplied to Acme Bank along with recommendations based on the observations made throughout the engagement, across technical, operational, and strategic areas.

Tooling

Acme Bank's EDR tooling showed limitations in response tasking, which slowed down the CSIRT's efforts to investigate the intrusion. Additionally, there was no response tasking enabling the organization to contain or remediate intrusions. This ability is something that becomes especially useful in modern networks that are geographically disparate, often with decentralized management of different assets.

The facilitators have both conducted engagements across a wide range of organizations, giving them insight into the capabilities of various tooling. With knowledge of such tooling – its nuances and the experience of using it in real-world incidents – they may provide insights for Acme Bank's strategic approach to procurement.

Roles and responsibilities

The composition of Acme Bank's CSIRT had been established at a high level when its IR plan was created, and its scope was limited to members of the security team. The simulation exercise showed resources and insights from other teams within the organization would be helpful, if not essential, during an incident. The report recommends other teams which may play a role during an incident are identified, and their representatives engaged during the planning phase. The CSIRT should further provide temporary membership for such representatives during a severe incident.

Training & skills

Acme Bank's CSIRT was known to be relatively inexperienced in dealing with large security incidents. However, its collaboration with F-Secure during the Response Process Development phase of the project provided them with insights into what to expect during an incident and how to prepare themselves accordingly. As the CSIRT grew in confidence in the second half of the simulation, they became more dynamic in their approach and more effective in providing solutions. This performance in a single session should encourage, rather than discourage, further investment in the team's capabilities through training and simulation.

The CSIRT's investigation team was able to provide high-level procedures for evidence collection and analysis during an incident when this became necessary during the simulation. When some of the details were challenged by facilitators, at least one member of the team was able to provide practical solutions.

In this simulation, all endpoint investigations had to be carried out manually, since tooling for remote response was not in place. The investigation team would be able to handle this for the head office and nearby branches, if endpoints targeted for investigation were carefully selected and prioritized taking current capacity into account. The exercise showed this would, however, not be the case for endpoints located in other regions, as getting personnel with the appropriate skills on site within a reasonable timeframe would not be possible.

Risk Management & documentation

The team was able to identify certain affected assets during the simulation, and contact the relevant owners based on a critical asset ownership roster that was started during the earlier phases of the project. This was still incomplete, and the team had to rely on memory and inference to identify others. The list of endpoints on which the attacker had a presence also included some critical business systems the team did not identify.

Completion and maintenance of a critical asset register, including interconnects and dependencies, is crucial to enable the CSIRT to effectively protect the organization during an incident. The simulation report recommends workstreams to identify these assets, define those most critical, and shape the overarching security strategy around them.

As touched on earlier in this paper, it is surprisingly common for organizations to lack appreciation of their critical assets, i.e. where the greatest impacts to their business could result from. The internal documentation an organization holds to define its critical assets, network, systems, and users is often inaccurate, despite the reality that modern threat actors will do their best to blend in with an organization's BAU activities. The documentation of these facts is therefore essential in supporting the identification of such threats, as well as providing critical context to technical investigation teams.

In a similar vein, the operational documentation for key contacts and ownership of assets or systems is often incomplete or non-existent. Uncovering this mid-incident can significantly slow down response efforts. Thus, designing a process to document these and keeping it up to date helps ensure response efforts are not hampered.

SUMMARY OF OUTCOMES AND CONCLUSION

Blue team engagements play an important role in ensuring organizations are prepared for incidents when they occur and can respond in the most effective way to reduce the inevitable impact.

In the case of Acme Bank, participants learnt much from the exercise, prompting a number of internal projects to help improve the readiness of the organization towards a real incident in the future. Simulation exercises are often useful for highlighting these additional required improvements and a good way to test the overall readiness of an organization for a real major incident.

Though this paper focuses specifically on blue team engagements designed to improve and assess response capability, they also cover preventative and detective security through strategic defensive consultancy and technical detection uplift respectively. As an area becomes more mature, the returns diminish, thus a spread of consultancy services across all three areas (detection, prevention, response) and targeted at an organization's least mature areas will often have the greatest return on investment (ROI). Running blue team activities as part of a wider rainbow teaming program ensures this happens.

The risk profile of an organization such as Acme Bank warrants the hiring of a technical security incident manager or resource to sit – as a continuous external resource – within the SOC to be the internal subject matter expert during incidents. A well-prepared, designed, and rehearsed response capability defined with a set of playbooks is an important part of an effective response strategy. It is not something that can be developed during an incident where time is at a premium, and the consequences of poor implementation may result in substantial financial and infrastructural impact to the business.

This is especially relevant in the modern threat landscape where enterprise ransomware attacks are increasingly common and have immediate and tangible destructive impacts to the prosperity of organizations. Investing in adequate (based on threats) response efforts in advance of an incident can have significant positive returns.

REFERENCES

[1] **Verizon 2019 Data Breach Investigations Report,**
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf

[2] **NIST Computer Security Incident Handling Guide,**
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[3] **CISA Cyber Incident Scoring System,**
https://www.us-cert.gov/CISA-Cyber-Incident-Scoring-System

F-Secure

www.f-secure.com/consulting