CHAPTER 9

Institute Resilience Through Detection, Response, and Recovery

Cyber-resilience provides the ability to withstand and mitigate the impacts of information risks. Businesses can start to become more resilient by identifying their critical assets, top risk scenarios, and basic contingency plans. Then, by aligning technical security capabilities with IT operations and other business functions, security leaders can enable the business to detect suspicious or anomalous events earlier, and respond and recover faster from incidents such as breaches or system outages.

Incident response (IR) is closely linked to security monitoring and detection. It should be managed by a dedicated group (or person) that coordinates closely with security operations, legal, HR, and other functions. Businesses should develop response plans for common types of incidents and for potential incidents from top risk scenarios. Enact response in a structured manner wherein each business function has a script for its part; for example, after a data breach, IT restores affected systems to normal operation, public relations communicates with the media, and the legal team notifies customers or partners of lost personal information.

Businesses can lay the groundwork to enable recovery from serious incidents by performing business impact assessments that identify critical assets and developing business continuity plans to restore or recover the assets. Recovery plans may overlap response plans in the case of cyber-incidents, requiring that business continuity teams and IR teams coordinate. Strictly operational incidents such as hardware failures fall purely in the purview of the business continuity function.

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_9

This chapter provides guidance for security leaders on how to

- Understand cyber-resilience requirements
- Address common resilience challenges
- Identify critical business assets, risk scenarios, and contingency plans
- Detect cybersecurity events consistently and promptly
- Respond to incidents
- Recover from incidents caused by cyberattacks and operational outages

9.1 Understand Cyber-Resilience Requirements

Businesses can achieve cyber-resilience by implementing smart risk management, robust security monitoring, and well-planned incidence response as well as business continuity/disaster recovery (BC/DR) programs that reduce cybersecurity breach impacts and/or operational impacts from IT outages.

Figure 9-1 illustrates cyber-resilience in terms of the NIST Cybersecurity Framework. “Identify” controls pinpoint critical assets, interdependencies, risks to the assets, and grant authority to defend them. All other cyber-resilience controls depend on this. “Protect” controls reduce probability of successful attacks. However, the probability of *any* attack getting through can rarely be reduced to zero. “Detect” and “Respond” controls can mean the difference between a cyberattack penetrating the IT environment but ultimately falling short of success and that same cyberattack materializing into a major breach. Incident response also sets the stage for recovery and business continuity.

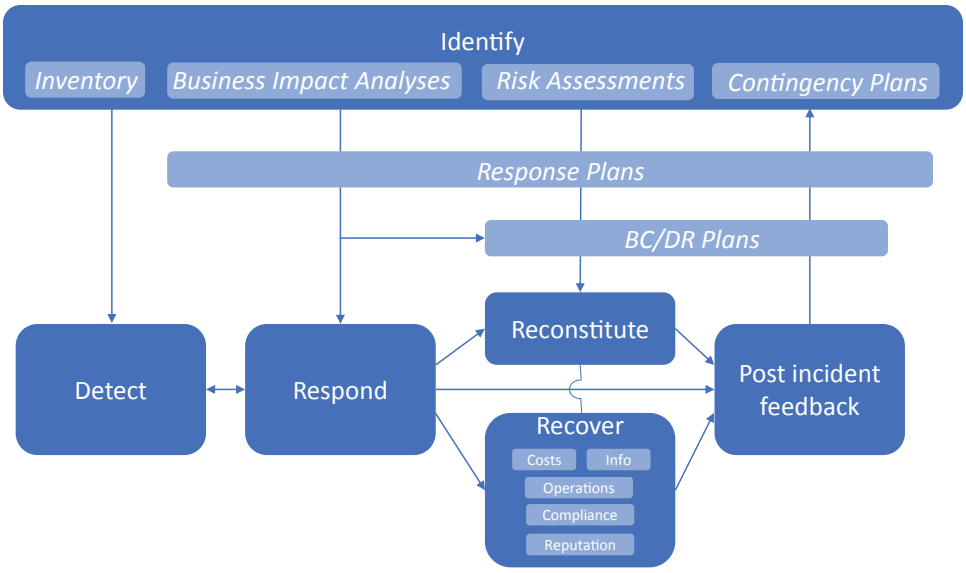

Figure 9-1. *A CSF-Inspired Cyber-Resilience Framework*

The following sections detail ways that Identify, Detect, Respond, and Recover controls can reduce the impact of cyberattacks and operational failures. They also describe good practices for aligning the technical work on controls with business stakeholders.

9.2 Address Common Resilience Challenges

Although Figure 9-1 charts a clear path to resilience, numerous challenges must be overcome. These include

- Business unpreparedness for response
- Lengthy cyberattacker dwell time
- Lack of visibility or access to all IT systems
- Difficulty hiring and retaining skilled incident handlers

9.2.1 Business Unpreparedness for Incident Response and Recovery

Most businesses have immature and/or underfunded incident response and recovery strategies and capabilities. They have not planned for, may not have experienced, and may not have retained staff who are knowledgeable about breaches of personal information, loss of trade secrets, outages, ransomware, or all the other types of incidents that can befall a digital business.

Above-average risk management, business continuity, and response processes are requisites for cyber-resilience. Without them, critical systems and their interdependencies may not be identified, detection is uncertain, recovery time objectives don't reflect business needs, and response or recovery could be ineffective. And yet according to surveys such as the FAIR Institute's "Road to Risk Management Maturity,"[1] the average overall level of risk management maturity was low at 33% in 2018.

Businesses in the 2020s will continue to face an elevated threat environment, with growing levels of automated malware attacks as well as, in some industries, nation-state attacks. Yet due to immature risk management and business continuity processes, they may not have their defensive priorities clearly focused on critical systems.

To monitor complex environments and investigate incidents, larger businesses may require both a security operations center (SOC) team operating 24x7 and a Computer Security Incident Response Team (CSIRT). Maintaining these capabilities at this level requires more than a dozen highly trained staff. Faced with these resource requirements, some try to get by as if they were much smaller organizations with just one person to perform the CSIRT role and SOC services during daylight hours only. What do you think happens when cyberattackers come in the night?

You guessed it – a breach (or its beginnings). Once the breach is discovered, the business lands in a maelstrom of trouble with technical, budgetary, customer, public relations, and human resources concerns colliding. Just when the need for cross-functional collaboration is at its highest, the organization is not prepared. No plans covered this type of incident, not even to specify who to notify or what to do. At best,

[1] "The Road to Cyber Risk Maturity 2018 Risk Management Maturity Benchmark Survey," FAIR Institute, January 2019

the incident becomes a huge distraction. Opportunity costs as well as response costs mount rapidly as executives call meeting after meeting to thrash through the issues and take hurried reactive actions. Inevitably they make some mistakes. If management also succumbs to internal infighting during the response process, the situation gets even worse.

9.2.2 Lengthy Cyberattacker Dwell Time

According to sources such as the "Verizon Data Breach Investigations Report,"[2] the average "dwell time" during which a cyberattacker can maintain a covert presence in an organization's digital systems before detection and eradication typically lasts for months. This can be disastrous because skilled attackers can progress from their initial beachhead to the target objective within minutes or hours,[3] and even lower echelon attackers have ample time to plan and attempt exploits.

Long dwell times offer attackers ample windows to exploit the victim organization's trade secrets, customer information, funds, or other targets. They enable observation and recording of individual or organizational activities to identify additional targets. Attackers have time to implant malware, backdoors, or logic bombs that assure their future access and ability to cause damage. And because criminals and spies can collaborate or share information on targets, other attackers may come in to "join the party" at the victim business's expense.

An organization could end up suffering multiple breaches, find some systems being used for botnet activity, others to mine cryptocurrency, and still more held for ransom. As soon as it fixes one breach, it confronts another. Without drastic measures to burn down and rebuild IT systems, the business could find itself in a state of continuous compromise.

Fortunately, businesses can take action to institute cyber-resilience along with our other priority programs and be leagues ahead of many of their peers and better prepared for many risk scenarios.

[2] "2019 Data Breach Investigations Report," Verizon, May 2019, accessed at https://enterprise.verizon.com/resources/reports/2019/2019-data-breach-investigations-report.pdf

[3] "2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed," Crowdstrike, March 2019, accessed at www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

9.2.3 Lack of Visibility or Access to All IT Systems

As we described in Chapter 7, many businesses have a fragmented IT environment spread across multiple operating units or international subsidiaries. These environments sometimes span complex hybrid cloud topologies over which they have poor visibility. The more fragmented the environment, the more difficult it is to establish centralized or coordinated security monitoring capabilities, log or event collection, and detection, response, or recovery services. Such difficulties arise due to both noninteroperable systems across silos of IT functionality and internal politics.

The larger and the more decentralized the business, the more political challenges complicate or kill security monitoring projects. Although a technical monitoring solution may exist, some units aren't forthcoming with data from workstations, network systems, or security tools such as secure web gateways or secure email gateways.

Technical immaturity in any of the following areas can compound political or IT interoperability issues:

- Incomplete monitoring infrastructure (i.e., lack of log collection or security information and event management systems (SIEM))
- Immature detection processes and alert triage
- Legacy antivirus (AV) solutions not well suited to investigative or forensic work

To remedy this problem, develop the capability to detect cybersecurity events consistently and promptly in critical systems and eventually to all systems in the IT environment.

9.2.4 Difficulty Hiring and Retaining Skilled Staff

According to surveys such as one from the Enterprise Strategy Group and the Information Systems Security Association International (ISSA),[4] over half of North America's organizations report "a problematic shortage of cybersecurity skills."

[4] "The Life and Times of Cybersecurity Professionals 2018," Enterprise Strategy Group and the Information Systems Security Association International (ISSA), April 2019, accessed at www.esg-global.com/esg-issa-research-report-2018

Anecdotal evidence from Rational Cybersecurity project interviews indicates that a shortage of skilled IR staff is a major gap; CIO James Rutt observed, "It's nearly impossible to source qualified IR professionals and retain them for long in the New York City area."

Even businesses that have staffed up find it difficult to satisfy and retain staff in security monitoring or IR roles over the long term. High skill requirements, a demanding work schedule, stressful incidents, and (in some cases) soul-destroying regulatory investigations make managing and retaining workers a constant struggle. Anton Chuvakin, a former Gartner Research VP and Distinguished Analyst who used to field multiple IR program inquiries from clients weekly, commented: "SOC managers tend to be chronically short-staffed and under pressure to fill entry-level positions with people who may be smart and dedicated, but are not yet trained."

Under these circumstances and in a hot cybersecurity job market, it isn't easy to keep one's best analysts happy and retain them in their critical SOC or IR positions. But failing to keep those functions staffed with trained people is a leading factor in security breaches.

9.3 Identify Critical Business Assets, Risk Scenarios, and Contingency Plans

The core processes for detection, response, and recovery depend heavily on identifying the critical assets of the business, their interdependencies, and the risks to those assets. IT and security leaders should conduct rolling business impact assessments (BIA), enterprise risk assessments, and cybersecurity maturity assessments at least every two years to provide a list of top information risks, a current state baseline, and a gap analysis of cyber-resilience capabilities. Contingency plans should be developed for how to perform response and recovery for probable types of incidents and outages.

9.3.1 Perform Business Impact Analysis (BIA)

A BIA is the first step in the business continuity planning process. Use BIAs to

- Identify a prioritized list of critical enterprise resources or services ("critical assets")
- Map critical assets to business processes

- Stipulate any legal and regulatory requirements for the assets
- Itemize interdependencies between the assets and other business systems
- Set goals for critical assets' recovery time objectives (RTOs)

The BIA focuses on identifying the impact to the business if a critical asset becomes unavailable. It specifies maximum acceptable downtime, or loss levels, and sets recovery objectives accordingly.

BIAs should normally be performed at least every two years. Meetings (typically 2–4 hours long) should be conducted by a business continuity (BC) professional[5] or someone trained in that discipline. The BIA lead should facilitate meetings with experts on each asset. The IT and security leadership must ensure that senior business stakeholders support the BIA as an objective, fact-finding exercise and that senior team members who work "hands on" with the services are in the room during meetings.

9.3.2 Analyze Top Risk Scenarios

Whereas the BIA identifies and prioritizes those assets or services most critical to the business, information risk analysis describes the top scenarios wherein threats exploit vulnerabilities to create adverse impacts of different kinds on the tangible IT assets identified in the BIA or on intangible assets such as brand reputation. As we wrote in Chapter 5, risk analysis is an ongoing process within information risk and enterprise risk management (ERM) programs.

A CISO's risk team should perform an enterprise risk assessment at least once every two years. As described in Chapter 5, section "Perform Enterprise Risk Assessments to Identify Top Risk Scenarios," the risk assessments should be aligned with the BIA but also look for top risks in other areas.

[5]BC professionals may be trained in the ISO 22301 standard and/or in industry-specific standards such as the Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook in the United States

9.3.3 Develop Contingency Plans and Cybersecurity Strategy for Resilience

Using the BIA and the risk assessment inputs, the IT and security organizations should prepare contingency plans for coping with outages, breaches, and other material incidents. The contingency planning process should draw information from the following work streams:

- **Cybersecurity maturity assessment:** Determine the organization's level of maturity at risk management, security monitoring or detection, IR, and BC/DR. What level of maturity and capability does the organization have currently, and what level should it target one or two years from now? Where are the gaps?
- **Incident response planning:** These plans (described in the "Respond to Incidents" section) will drive IR procedures for different types of incidents and must be created through an iterative capability building and learning process.
- **Business continuity planning:** These plans (summarized in the "Recover from Incidents Caused by Cyberattacks and Operational Outages" section) will prepare the ability to recover systems that have been damaged in breaches or outages.
- **Cyber-insurance coverage acquisition:** Chapter 5, section "Treat Risks Holistically," suggests cyber-insurance as a means of risk transfer under certain conditions. Based on the business's top risks, business leaders from the finance, legal, IT BC/DR, and security functions can work closely together to obtain the right kind of cyber-insurance policy and conduct operations to preserve the organization's eligibility for coverage. Because some cyber-insurance policies require the business's IR function to coordinate with the insurance company's breach responder, any constraints and opportunities from the actual cyber-insurance policy must be factored into IR contingency plans.

Contingency plans for cyber-resilience should be part of a business's IT and security strategies. IT and security leaders can recommend ways for business risk owners to deal with IT failures or incidents arising from strategic risks. The actual plans can summarize and reference existing and more detailed risk registers, IR plans, and BC/DR plans. If none are yet developed, the contingency plans can develop preliminary assumptions and starting points for them.

Once the business has a maturity assessment covering the cyber-resilience functions, IT and security leaders should work with business executives to set direction on three key cyber-resilience decisions considering the business's maturity level and future needs:

- **Roles and responsibilities:** Who is responsible for security monitoring? Incident response? Recovery of various types of systems? Accountabilities must be identified among executives, business process owners, CIOs, and CISOs and responsibilities or consultations to the CSIRT, SOC, business continuity team, service managers, and others.
- **Security monitoring – organization and staffing:** Does the business need a SOC with 24x7 coverage? A 24x7 SOC requires 8 to 12 highly skilled (and expensive) staff. Alternatively, the organization could stand up a "SOC lite" with fewer persons but reduced hours. It could use managed security services providers (MSSPs) and managed detection and response services (MDRs) that provide round-the-clock services to augment small (even one person) in-house security monitoring teams. However, outsourcing security monitoring requires careful management, and it may reduce the business's ability to cover all locations and to tailor detection to its unique applications, configurations, people, and processes.
- **Computer Security Incident Response Team (CSIRT):** Where does the CSIRT function reside in the organization? In larger businesses, different groups should provide security monitoring and CSIRT functions. However, technical staff and duties overlap. The CSIRT also requires support from nonsecurity stakeholders, such as legal, human resources (HR), marketing, PR, and others.

9-1

Because cyber-resilience requires considering business drivers, top risks, risk appetites, and IT security governance questions get as much input on the strategy as possible from executive management.

"Everyone has a plan until they get punched in the face."

Mike Tyson

9.3.3.1 Plan for Unexpected Incidents

Many incidents fall into known types. Even if some of the details of threats, impacts, and response or recovery strategies have to be discovered or developed on the fly, existing playbooks for the incident type provide a place to start.

Completely new types of incidents could throw the CSIRT, the CISO, and the whole company into a state of chaos or panic. Businesses in some industry sectors, such as the retail clothing, might reasonably expect to never encounter a nation-state attacker (aka advanced persistent threat (APT)). Suppose, now, one of those businesses receives forensic evidence from their national intelligence agency that indicates it has just experienced its first APT attack. What should the business do now, and how could it have prepared?

I hate to say this: Preparing for unexpected incidents requires having a "plan for a plan." This needs to be one of the CSIRT's playbooks and a subject for training exercises. Part of stakeholders' orientation to their role in the CSIRT should state that "If you get a meeting request with a subject line such as 'Urgent: Critical New Incident Planning Meeting,' you attend that meeting." Such meetings could have a simple objective to create a playbook on the spot, at a minimum identifying

- An incident commander and accountable executive(s)
- An incident team
- Internal or external resources to draw on (in our example) to come up to speed on APTs very fast

- Any existing playbooks (from other incident types or provided by vendors or security information groups) to use as template or starting point
- Next steps

9.3.4 Develop Business Continuity and Disaster Recovery Plans

Preparing a business continuity plan helps the business recover quickly if an incident does happen. Although it isn't possible to predict every kind of incident that could threaten the business, one can develop plans that cover a range of incidents (e.g., natural disasters, computer problems, staffing issues, pandemics). A business continuity plan helps to identify and prevent risks where possible, prepare for risks that can't be controlled, and respond and recover if an incident or crisis occurs. The size and complexity of BC/DR plans depend on the size and type of business, but IT and security leaders and service managers should ensure that they include

- Information required to recover from catastrophic failures, to get the business running again
- Procedures for restoring critical systems or applications within defined recovery time objectives
- Periodic testing of recovery processes
- A schedule for updating the plan itself to account for any changes to the business, the industry, or the operating locations

9-2

Ensure that senior business stakeholders support the business continuity program and that the key IT team members who work "hands on" with mission-critical services are in the room during BIA and BC/DR planning meetings.

Some companies routinely purchase extra capacity (e.g., 25% above current demand) to all IT procurements as cyber-resilience requirement. Occasionally such procurement policies pay off. For example, over-provisioning spare notebook computers and remote access solution capacity would have made businesses more resilient

to the COVID-19 pandemic. In general, BCP/DR plans should also be informed by requirements to provide cyber-resilience in the event of infrequent but high impact events such as hurricanes, prolonged power outages, and pandemics. BC/DR team members should be informed of these scenarios by the risk management team and (since they are infrequent) devise ways of increasing resilience – whether by design, procedural contingency plans, or incremental capability – that don't add much to cost but do leave the business better prepared. Rather than overstocking licenses and VPN gateway appliances, for example, a pandemic prepper could arrange and test cloud-based remote access capacity for use during crisis or peak demand periods.

9.4 Detect Cybersecurity Events Consistently and Promptly

Per the NIST CSF, "Detect" controls must backstop "Protect" controls. Businesses must collect logs, generate and receive real-time notifications, and investigate events which could be indicative of security problems. Detecting advanced (or stealthy) threats requires more sophisticated monitoring tools and processes, skilled staff, and enough event context to distinguish normal from malicious activity. Monitoring capabilities must be deployed in all IT domains (i.e., on-premise data centers, end user networks, cloud infrastructure, and applications). Outside the enterprise IT systems' domains, businesses should also monitor user feedback to the company as well as security-related notifications from external parties.

Security monitoring systems process information and analyze it to find indicators of compromise, precursors to attacks, or vulnerabilities. A good monitoring infrastructure will detect many issues, most of which are unimportant, repetitive, or false alarms. Security monitoring can be like looking for needles in the haystack, such as

- Threats, human or automated, attacking or already inside the systems
- Security controls not operating in compliance with policy
- Information assets that are missing or failing to pass security tests or health checks

9.4.1 Monitor Event Logs, Alerts, and Reports

First, we must capture the data! Basic event logging gives visibility of IT and security-related activity, establishes baselines for normal activity, and provides data for an audit trail. Monitoring and logging processes and tools must cover log creation, collection, and management as well as real-time notifications to security consoles, operators, or tools.

Security teams can employ log management and SIEM tools to collect logs and events. The tools can understand and normalize many kinds of log data from different systems (such as security systems like firewalls, endpoint protection systems, and directory services) as well as server, application, and endpoint resources. However, standards are required for custom applications' logging and alerting function and for configuring off-the-shelf systems.

After collecting log data, alerts, and notifications, businesses can run this information through automated analysis, perform human log review on selected issues, and retain certain log records. If we could capture all the events in the enterprise that are meaningful to IT and security objectives, it would be as if these events were pouring into a giant funnel for filtering, refinement, and processing.

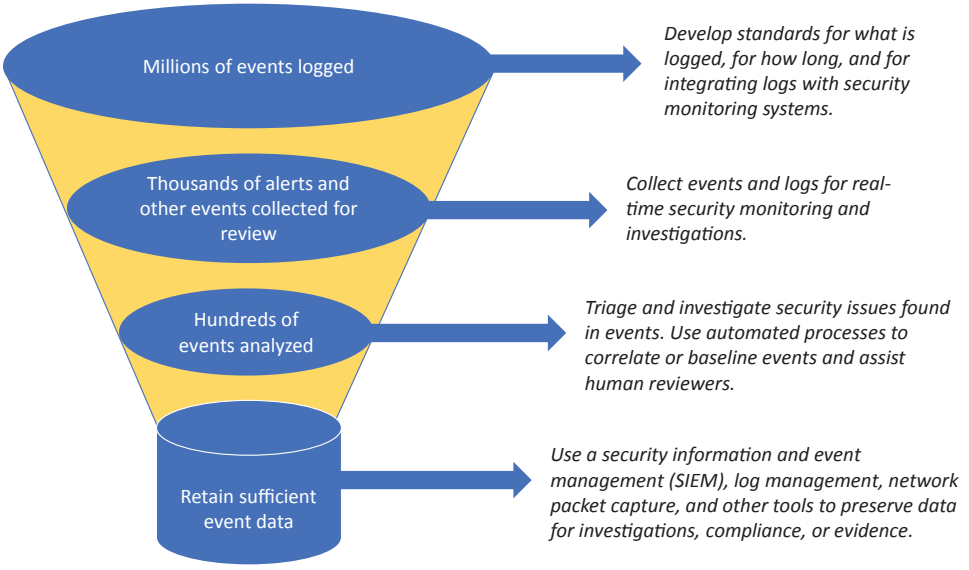

Figure 9-2. *Log and Event Data Generation, Collection, and Processing*

9.4.1.1 Collect Data for Investigations, Retain It for Compliance and Evidentiary Purposes

Many logs collect IT and security data. Even for a small business with less than 100 employees, the security department should be monitoring the firewall, endpoint anti-malware, directory services, email server, and production web/commerce site logs. Use log collection tools to collect some or all the logs' information to a central server. Tool options range from open source Logstash and Elasticsearch to perform basic log collection at the low end all the way to enterprise class SIEMs from vendors such as Splunk, IBM, RSA Security, and others.

A good log collection tool should have some default settings for which events to collect and which to drop. Businesses should generally take advantage of the tools' capabilities to normalize, summarize, or compress events to increase capacity. However, in some cases, business, security, and legal departments should also retain raw logs for evidentiary and forensics use against attackers.

Log data can accumulate fast, even with summarization. To avoid storing too much or too little, work with the legal and compliance functions to set data retention requirements where they apply for critical systems or regulated systems. Even where no regulatory retention requirements exists, note that the longer the retention period, the longer the lookback period available for investigations. For example, suppose we find a hacker penetrated the organization's systems at least two months ago; full network packet capture systems can prove invaluable in tracking down which systems were compromised and which external command and control sites were used in the attack.

9.4.1.2 Use Context to Enrich Events

To avoid generating too many alerts, or false positive alerts (e.g., on *every* instance of multiple login failures to a user account or *every* attempted hack against a server), SIEMs and other tools can automatically correlate events from multiple log and notification sources to gain additional confidence that something is wrong or to prioritize among the many potential issues. For example, a SIEM could prioritize an alert about a system logging port scans (indicative of hacking interest) if the SIEM also learns that said system is

- An executive's laptop (context source: Active Directory)
- A server with unpatched vulnerabilities (context source: vulnerability scanner)
- A server in the scope of Sarbanes-Oxley (SOX) audits (context source: asset management system

In short directory services, vulnerability management systems, asset management systems, and many other IT security capabilities can provide context to the SIEM or other monitoring tools. Monitoring tools can also use enterprise context information to enrich events and reports with additional information. Keeping context information accurate, up to date, and accessible is a critical success factor for effective security monitoring. Security engineering resources can be dedicated to integrating monitoring tools with context sources.

9-3

Identify IT or security administrators responsible for context sources and engage them in efforts to improve security monitoring capabilities.

9.4.1.3 Automate Monitoring Tools, Processes, and Use Cases

Collecting all the logs and notifications in the world is useless unless the organization reviews the information and investigates and acts when necessary. However, given the high volume of events even in a small organization, human log review can become an insufferable burden. Although required in many cases, it should be supplemented by automated detection systems.

There's a wide spectrum of tools and approaches to automated review. At the low end, security staff can develop in-house tools and scripts to search or summarize log information. We can hire an MSSP to monitor our networks, firewalls, and other systems or logs we give it access to; the MSSP will certainly employ automated log review and analysis on our behalf. We can also obtain a SIEM. At the high end of automated review, we can invest in automated machine learning and other security analytics techniques. Other advanced types of tools include network traffic analysis (NTA), anti-malware sandboxing, data leakage protection (DLP), user entity behavior analytics (UEBA), privileged identity analytics, database activity monitoring (DAM), and more.

A large organization generally employs multiple approaches. It may retain an MSSP to monitor its firewalls and externally facing systems, leverage cloud-native tools such as the Microsoft Azure Security Center, and use a SIEM to monitor internal systems. Also, groups responsible for mission-critical custom applications or specialized tasks such as running DLP may develop homegrown scripts to parse through the logs or customize a general-purpose SIEM. For organizations that have limited budgets or lack most of the tools noted here, there is an opportunity to combine some security monitoring use cases (such as detecting login failures and certain types of vulnerabilities) with IT operational monitoring for service availability or early warning of logical or physical system failure. Automated tooling for operational monitoring can provide a rapid entry for automated security monitoring.

With so many events that could be monitored, businesses need to focus on important use cases such as

- **Monitoring critical assets**, such as *any* suspicious events on a large credit card database
- **Monitoring controls** to prove they are operating correctly for compliance or assurance purposes
- **Monitoring activity against a baseline for anomaly detection:** For example, alert on record spikes in network activity or root administrator access to servers from unusual locations at unusual times

Prioritize developing those use cases that solve the most critical issues or easy ones that have some value to implement. Also prioritize use cases that improve the security monitoring group's capability (e.g., developing a new context source, log integration, monitoring tool capability, or staff skill).

9.4.1.4 Use Human Review to Supplement Automated Systems

Automated monitoring capabilities such as the use of artificial intelligence (AI) in security analytics may seem more glamorous, but the human element continues to comprise an important part of security monitoring. What security teams need to do is *progress from tedious and repetitive log review to tuning and backstopping automated systems*. Human expertise is required to

- Review logs and notifications for indicators that can't (yet) be automatically detected and spot check that automated systems are detecting what is expected
- Provide compliance signoff that logs have been reviewed manually and/or that automated monitoring is operating as intended
- Detect new threats or control failures that haven't been instrumented for automated monitoring
- Complete deployment of automated monitoring use cases and fine-tune them
- Provide human oversight of monitoring change control processes

During early maturity stages, businesses tend to rely more heavily on manual review. Logging standards should include provisions for human log review. In addition, operations runbooks, or procedures, should contain checklists for administrators to verify that all monitoring capabilities are functioning. Looking forward, human expertise is also required to develop automated monitoring use cases.

9.4.2 Investigate and Triage Real-Time Alerts and Issues Found in Logs

By Murphy's law ("What can go wrong, will go wrong"), once the organization begins logging, generating notifications, and performing automated or manual review, many issues get raised. But how does the organization determine which need action and what to do with them?

Issues from security monitoring may fall into the following classes, and the monitoring team should have instructions on what to do with each as shown in Table 9-1.

Table 9-1. *General Security Monitoring Instructions (SAMPLE)*

What to Monitor	What to Do
Precursors to compromise, such as cyberattacks in progress	Investigate and/or escalate to CSIRT team
Indicators of compromise	Investigate and/or escalate to CSIRT team
Signs of control failure	Notify appropriate security operations support team
Signs of system failure	Notify appropriate IT operations support team

Issues relating to indicators of compromise or precursors remain with the security monitoring function and/or the IR function for further investigation and triage. As we'll discuss in the "Respond to Incidents" section, businesses have different approaches for dividing work between the security monitoring and IR functions. Events requiring investigation can go into a "response identification" queue. Some issues should also go to the tiered risk assessment process discussed in Chapter 5.

9.4.3 Modernize and Scale Detection for Distributed Infrastructure

A White Paper for Rain Capital[6] takes us to the frontier of automated detection in widely distributed public or private cloud infrastructure and application architectures. These architectures, especially when combined with ephemeral workloads or services, challenge traditional static security approaches. Detection must be automated, decentralized, distributed to the cloud-native control plane, adaptable to changing service fabrics, and instrumented with response capabilities.

[6]"DevSecOps and Detection Engineering: New Approaches to Security," Jamie Lewis, Rain Capital, December 2018, accessed at www.raincapital.vc/resources

DEVSECOPS AND DETECTION ENGINEERING: NEW APPROACHES TO SECURITY

"Technical solutions for problem detection in distributed architectures require new security solutions. These solutions require real-time visibility and iterative feedback loops for security measures to adapt continually to rapidly changing environments and conditions. Automated detection engineering must be built in to take continuous measurements and make real-time adjustments.

The emerging practice of security chaos engineering proactively probes for failures in security controls through controlled experiments such as randomly shutting down an instance or changing a protection setting. These experiments can be "controlled" in the sense that they occur within a limited blast radius and test failure modes the system is already supposed to cope with. Still, we recommend they be closely-supervised by skilled engineers and DevOps teams."

Jamie Lewis, Venture Partner

Lewis also wrote that detection engineering in distributed architectures involves decentralizing operational security roles and functions. These conclusions align with those from Chapter 7, section "Upgrade IT Operations with DevSecOps and Disciplined Agile." For business building or running large-scale distributed infrastructure, detection engineering and security chaos engineering could become core competencies and require alignment between skilled security, IT, and application engineering teams' resources.

9.4.4 Hunt for Threats Proactively

Considering the "dwell time" survey findings discussed in the section on "Address Common Resilience Challenges," businesses desperately need to overtake cyberattackers. Knowing that in large, complex enterprise environments some threats are probably always present, businesses under regulatory and security pressure should consider maturing their detection processes to proactively hunt for incidents in what is almost a continuous process of investigation and response.

Threat hunting doesn't just require tools (such as UEBA, advanced security analytics, etc.). It requires skilled and dedicated personnel to

- **Increase investigation frequency and cadence** to hone capabilities and anticipate adversaries
- **Perform periodic indicator sweeps** to find specific indicators or precursors of compromise based on threat intelligence such as suspect insider activity, suspect IP addresses or accounts, or malware types and configuration anomalies seen at compromised organizations
- **Pivot or "clone" a hunt** when searching for one indicator leads to signs of other indicators or precursors

9.4.5 Coordinate Detection with Users, Business Stakeholders, and External Parties

An organization's IT systems, their logs, and their notifications may be the most important information sources for detection, but by no means the only sources. Security organizations can develop a Threat Actor Library (see Figure 9-3) identifying the categories of threat agents most motivated to attack the business and also analyze the types of threat events such agents could (or already have) created.

9-4

Engage knowledgeable internal and external sources to understand the risks and early warning indicators of compromise from each type of threat.

As they break threats down by category, and classify threat actions as shown in Figure 9-3, security and risk analysts can find many opportunities to improve detection by aligning with knowledgeable internal and external sources. Engage human users as sensors and develop processes for obtaining specialized security tips from other departments (such as HR, procurement, or facilities). Analysts should also take advantage of third-party security monitoring information or notifications and obtain threat intelligence from security information sharing bodies.

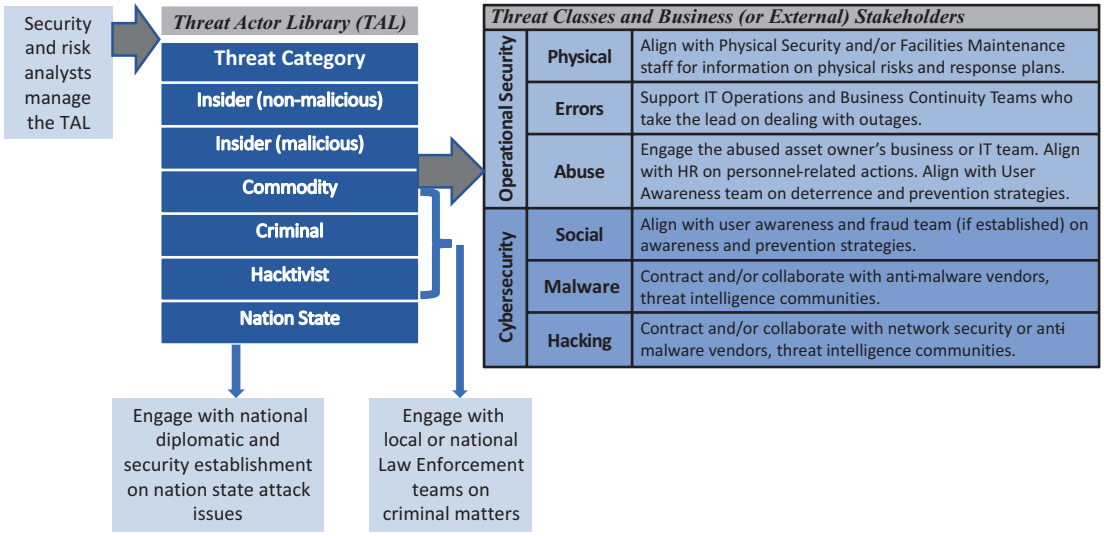

Figure 9-3. *Aligning with Business and External Stakeholders to Detect and Respond to Threats*

9.4.5.1 Engage Human Users as Sensors

IT users, developers, business users, partners, customers, or even someone in the general public – that is, anyone outside the security organization itself – may be the first to notice something unusual in the IT environment or pick up on some other threat to the organization. In the case of social engineering or physical attacks, human intelligence ("humint") may be the only notification source.

Establish well-publicized ways for users to contact or notify the security team about issues they observe. Notification methods can include ticketing systems, contact email addresses, and web forms. There may be a public-facing security contact mechanism. The security organization should also focus awareness training on IT or customer support functions (such as help desk and sales account representatives) to encourage such staff to look for security issues and report them through the notification process.

9.4.5.2 Develop Collaborative Processes with Business Functions

In addition to using IT or customer support functions as notification intermediaries, security functions should work with other corporate administration functions such as HR, physical security, third-party risk management (TPRM), facilities, and sales to obtain early warning of security issues (or even risk scores on individual users, vendors, or facilities) as follows:

- **Legal and HR** may be the first to see early indicators of insider risk, such as formal disciplinary actions and complaints against staff. At a minimum, HR staff (or an employee's manager) should give the security organization a "heads up" about certain types of issues with key users, e.g. a highly privileged IT administrator being formally disciplined. Consult the legal department, however, before monitoring or profiling internal staff. The rules may vary by jurisdiction and based on whether monitoring targets the user's personal device or a company-issued device.
- **Sales, marketing, research, and other business functions** are the data owners and risk owners. They are often best positioned to identify sensitive data and decide when to block use or transfer of sensitive data.
- **TPRM or vendor management** should track negative press reports, financial reports, or complaints about suppliers or partners as a matter of course. At a minimum, it should notify the security organization when a vendor is in the process of being terminated.
- **Facilities teams** should track break-ins, reports of thefts, and other issues with facilities and make the information available to the security organization.
- **IT and development functions** are well positioned to discriminate alerts that are harmless anomalies from those that are precursors to compromise. One CISO we interviewed described a practice of holding contests[7] for IT and security staff to develop original

[7]"Crowdsourced Splunking for Security Exploits," Dan Blum, November 2014, accessed at https://security-architect.com/crowdsourced-splunking-for-security-exploits/

correlation rules for the Splunk SIEM tool. Correlation rules had to use data from two or more logs, at least one of which was not under that author's control.

- **Vulnerability disclosure intake and bug bounties:** Provide an easy-to-find web page and other contact points through which "white hat" vulnerability researchers, law enforcement personnel, and vendors can submit bug reports for custom business applications or tips on potential threats to the business.

Information from these sources should be evaluated by security monitoring or IR teams in case it poses immediate risk. In some cases, it should also go to the organization's information risk team.

9.4.5.3 Integrate Workflows and Notification Processes with Contracted Detection Services

Contracted detection services – such as full-service MSSPs that monitor selected networks and applications and cloud security services like Azure Advanced Threat Protection or AWS GuardDuty – have useful capabilities, but rarely cover an organization's full IT environment. When outsourcing security monitoring tasks, businesses must coordinate closely with the vendor on monitoring and investigating

- Internal areas that are difficult to instrument for MSSP sensors (e.g., custom applications) or highly sensitive (e.g., executive workstations and devices)
- Keeping MSSPs or cloud vendors up to date on asset disposition, points of contact, and other enterprise context information
- Coordinating alert triage or investigation and remediation workflows with vendors
- Jointly developing, maintaining, and testing new monitoring use case capabilities
- Monitoring MSSP or CSP performance against SLA's and other contractual obligations

9.4.5.4 Obtain and Share Threat Intelligence from Security Information Sharing Bodies

Threat intelligence (TI) is especially important for businesses within industries under high security pressure – such as financial services, government, or critical infrastructure. Examples of information sharing bodies include

- Security vendors and other organizations providing open source intelligence or providing threat telemetry for a fee
- Other vendors or partners reporting incidents or breaches they have experienced in their environments, or from your organization, either proactively or under contractual obligation
- Vulnerability researchers disclosing vulnerabilities or exploits (perhaps in response to the organization's bug bounty program)
- Industry Information Sharing and Analysis Centers (ISACs)
- National Computer Emergency Response Teams (CERTs)
- Law enforcement organizations

In its Computer Security Incident Handling Guide (SP 800-61),[8] NIST advises that organizations plan coordination with external notifiers and information sharing organizations in advance. The security organization can work with "coordinating teams" such as US-CERT or an ISAC for the relevant vertical industry. Businesses should also develop communication guidelines for sharing their own information with external parties. Often, sharing technical information such as a suspect IP address or malware sample is low risk and helps establish the organization as a valued member of the information sharing community (and thus making it more likely to receive higher-quality TI). Sharing information about incidents that might have to be reported as breaches, certain kinds of control failures or security configuration information, and any user identity information should only be done with business and legal guidance.

[8]"Special Publication (SP) 800-61 Rev 2 Computer Security Incident Handling Guide," National Institute of Standards (NIST), August 2012, accessed at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

9.5 Respond to Incidents

Most businesses have an underdeveloped and underfunded IR capability. Yet ironically, the ability to interrupt a cyberattack on the organization's crown jewels, or even just provide a satisfactory response to an already large breach, could easily pay the full costs of a multiyear IR program.

Just as police must be able to solve most murder cases within the "first 48" hours, security responders need to stop or contain the spread of potentially dangerous cyberattacks within the first hour or even minutes. I spent considerable space in the previous section on Detection, which is the prerequisite to Response, and I'll refer between these codependent functions often.

With that, let's look at how to plan, establish, and evolve a well-planned phased response model, such as the SANS Institute's six-step process[9] shown in Figure 9-4, for many types of incidents.

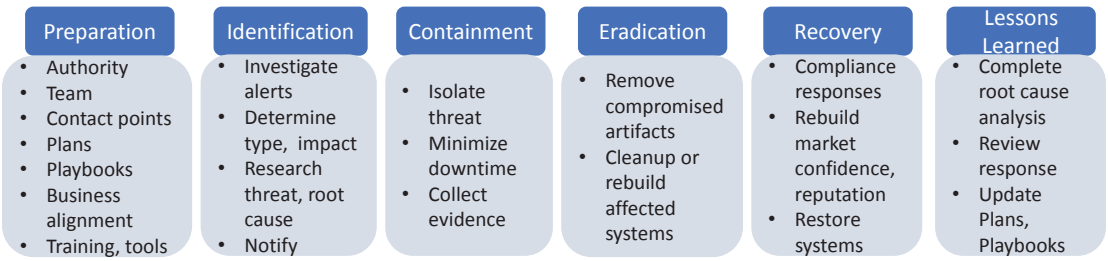

Figure 9-4. *The Phased Response Process*

9.5.1 Plan for Incident Response

Recall from the "Develop Contingency Plans and Cybersecurity Strategy for Resilience" section that the cybersecurity strategy should set directions for both IR and monitoring as well as for outsourcing to MSSPs and breach responders. However, detailed IR procedures for different types of incidents must be created through an ongoing process. Start by crafting an initial response plan that defines types of incidents, provides general guidance and objectives for responding to them, establishes lines of authority or decision rights, and organizes a robust IR function.

[9] "Incident Handler's Handbook," Patrick Kral, SANS Institute, February 2012, accessed at www.sans.org/reading-room/whitepapers/incident/paper/33901

Define: What is an "Incident?" Per NIST SP 800-61: "An information security incident is a violation or imminent threat of violation of data or computer security policies, acceptable use policies, or standard security practices." For example, finding malware on a production server, getting a report of a lost company laptop, or discovering unauthorized accounts, data transfers, or applications (such as cryptomining) would all be considered incidents at many businesses. Security leaders should identify common types of incidents and others that correspond to the business's top risks.

Provide guidance: How should the business respond? The business should already have direction on key staffing, outsourcing, and target IR maturity level decisions. Now it's time to expand the strategy into detailed response plans. Develop plans for a phased response for each type of incident. (Consider one objective: *Quickly eradicate malware using device reimaging tools and get staff working again.* This requires strong backup and restore capabilities, but may trade off most efforts at forensics, evidence gathering, and prosecution to a later time when the IR process becomes more mature.)

Establish authority: Who is in charge of the IR function? Continuing at the most basic level, businesses must designate lines of authority for coordinating IR functions and leading the IR team. Considering basic types of incidents, responses, and impacts, what does the IR function have authority to do (e.g., monitor user accounts, shut down production servers, cut network links, call vendors or partners, notify law enforcement) and under what circumstances? IR authorities and responsibilities vary with the type of incident and are highly contextual to location and other factors. For example, IR leaders may be required to notify law enforcement immediately on discovering threats to human safety and child pornography on a company system but in all other cases defer law enforcement notification to the Corporate Counsel.

9-5

Establish an incident response team to prepare response plans with business executives, legal, HR, vendor management, and public relations. Coordinate their responses during a breach.

Organize IR team: How can we build and maintain a healthy IR function within a security operations team? Security monitoring, technical response, and CSIRT functions require different – though overlapping – staff, skill sets, and personalities. Security monitoring can be somewhat repetitive and predictable, a

stable job. Technical incident response activities are more dynamic and exciting. CSIRT leaders must be able to play the politician, gain support for recovery or response internally, and be prepared to deal with law enforcement, the media, and irate partners or customers.

Figure 9-5 diagrams the interrelationships between the security operations functions supporting IR. The "resource flow" arrows show that although three different functions should exist in security operations, they must all support IR. Very few businesses permanently retain enough staff to cope with major incidents, so IR will tax all security operations functions whenever major incidents materialize.

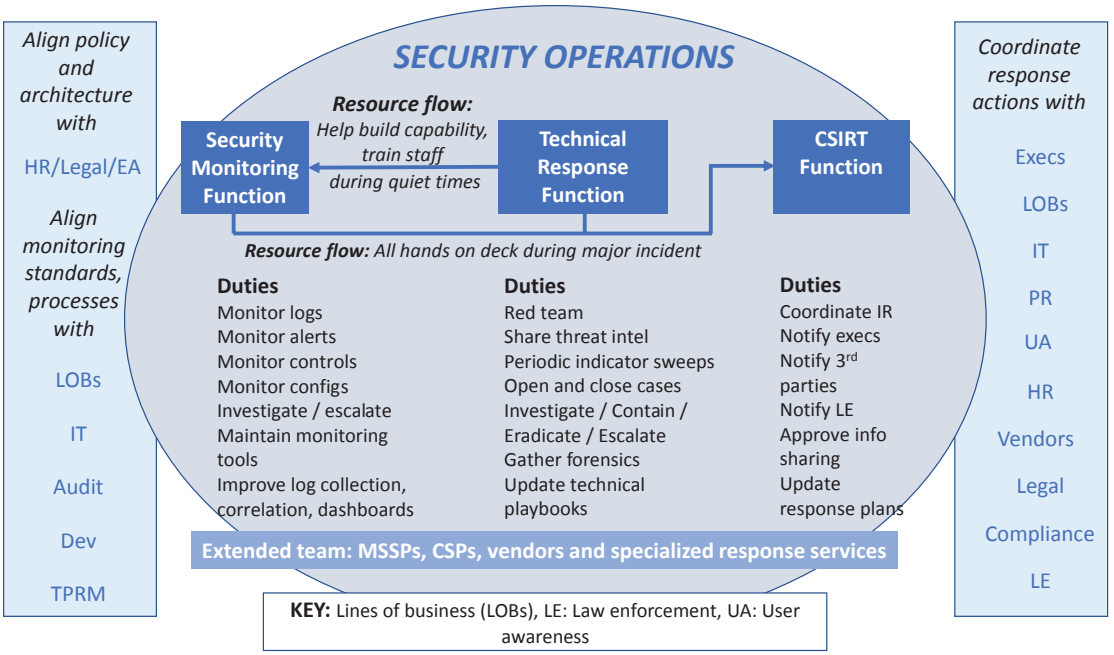

Figure 9-5. *Security Monitoring, Response, and CSIRT Functions*

Just as security leadership must align with the business before and after IR to prepare and coordinate, it must organize itself to endure the IR resource demand peak that occurs during major incidents. However, security leaders must also be aware that the effects of major incidents can persist for some time, especially in the event of legal issues, regulatory investigations, or repeated cyberattacks. With many security teams already under-resourced or under stress, take care to avoid excessive staff burnout and attrition.

Correctly structured, security operations can

- Give burned-out responders a rest when they can be spared; they can train others, update documentation, or work on automating monitoring processes
- Move bright but still junior monitoring staff seeking career advancement into the breach to augment responders during a major incident
- Provide learning opportunities, travel, conference tickets, appropriate time off, and reasonable work-life balance accommodation to all staff
- Work with the teams on developing job improvement strategies, response plans, and playbooks to give them the sense of efficacy that only a well-planned security program operating according to its plan can bring

Consider the guidance from Chapter 2, section "Hire, Motivate, and Retain Key Security Staff," to be especially pertinent for the security operations and CSIRT teams.

9.5.2 Establish the IR Program

Based on the cybersecurity strategy and the initial response plans discussed so far, the business can establish a full set of IR policies, plans, and procedures as well as build out its security operations teams to cope with the ebb and flow of incidents.

Regardless of organization size, a business must prepare for response by specifying policy, identifying points of contact for incidents, and designating a response team. Establish relationships with external IR resources, such as law firms specializing in different types of incidents as well as expert cyber-breach responders on retainer.

Policy: Formalize response plans in a policy identifying IR authority, purpose/objectives, scope, definitions and prioritizations, and basic team structure as well as guidelines for escalation, coordination with external entities, information sharing, and performance metrics. Because recovery should follow response, IR policies must be kept in sync with business continuity plans and policies.

Processes: Establish processes under the policy guidelines for escalation, case management, phased incident handling, and information sharing. Coordinate process development for dealing with suspected insider abuse, law enforcement, media, customers, partners, and facilities with HR, legal, public relations (PR), marketing, and facilities management groups, respectively. Design processes as living documents

implemented through continuously evolving security operations, CSIRT, and IT or development procedures and playbooks.

- **TIP:** Recognize that the CSIRT and security operations functions have major dependencies on the business functions identified in Figure 9-5's sidebars as well as on IT help desk or support and other security specialists. Build business alignment integration points to fulfill these dependencies into processes and procedures. Strong management and communication skills are required for the CSIRT to coordinate with multiple groups affected during incidents. Organizations under high security pressure should provide role-specific awareness training throughout the business to prepare staff for IR needs.

Staff up: All but the very smallest businesses should have the three distinct security operations functions shown in Figure 9-5. The number of staff providing security operations and IR can range from a pair of employees with several roles covering all three functions to multiple teams totaling many more than 20 people for very large businesses with 24x7 SOCs and per-incident leaders in the technical response and/or CSIRT functions. Ensuring sufficient resources are available to provide coverage for all three functions is critical; otherwise IR outcomes, staff retention during long-running incidents, and the ability to continue normal monitoring to head off further incidents could all be negatively impacted.

- **TIP:** Retain enough staff to handle the security monitoring workload plus technical response to ongoing incidents such as malware remediation, system restoration, and lost devices. Consider combining internal monitoring and response with a robust MSSP to reduce the need for in-house staff. Employ a core CSIRT team and (if risk warrants) technical response staff experienced in threat hunting. Institute job rotation and cross-training to get the best "mileage" from the security operations and CSIRT staff. Consider retainer contracts for specialized cyber-breach responder resources for further staff augmentation during major incidents.

Tool up: Most of the tools required are security monitoring tools identified in this book's Glossary, such as SIEM, UEBA, DLP, anti-malware, and others. IR also requires a case management tool. At the low end, an ITSM tool can track incidents. However, specialized case management tools provide more IR-specific functionality, such as forensics support and connections to threat intelligence sources. At a minimum, ensure that IT help desk and

other support staff outside the CSIRT cannot access sensitive incident information. Finally, don't forget that responders need adequate resources such as documented playbooks for common incidents, standard *and* investigative workstations and laptops, private conference rooms, redundant and protected communication methods, baseline virtual machine files available to quickly reimage or restore systems, and more.

9.5.3 Evolve the IR Program for Cyber-Resilience

The IR program is the centerpiece of cyber-resilience in the sense that it not only embodies Respond controls but also interacts with Detect and Recover controls. Response requires Detect controls to identify the threat (triggering response) and to verify containment and eradication. Then, Response initiates Recovery.

Businesses can evolve cyber-resilience capabilities up to Level 3 maturity (Defined) by creating contingency plans, IR policies, processes, and playbooks as well as basic automated monitoring capabilities. Level 3 IR already requires expanding staff, establishing the dedicated IR function, and spreading awareness of basic IR plans, roles, and responsibilities to security, business, and IT stakeholders.

Businesses under medium security pressure should consider – and those under high security pressure must – attain at least the Level 4 maturity (Managed) for security monitoring and IR. Getting to Level 4 requires yet more advanced tools and processes, including context- and correlation-enabled automated detection, alert investigation/triage, threat intelligence sharing, staffing a dedicated response function, and implementing all defined cyber-resilience processes more comprehensively across the business.

As the IR program evolves to Level 3 or Level 4 (Managed), it can develop the skills, resources, and playbooks for incidents the organization expects to eventually experience, as well as frameworks to address unexpected incidents. Conduct simulated incident exercises to prepare staff. Ensure response capabilities cover multiple IT environments including private clouds, public cloud such as AWS or Azure, and enterprise applications or SaaS. In some cases, CSPs such as Amazon[10] or Microsoft Azure[11] provide cloud-based detection and response tools and processes; customers should use these capabilities but must keep driving the response process themselves.

[10] "AWS Security Incident Response Guide," Amazon, June 2019, accessed at https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

[11] "Tutorial: Respond to Security Incidents," Microsoft, August 2018, accessed at https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-incident

Standard operating procedures or playbooks for incidents should describe in detail how to identify, contain, and eradicate the incident-inducing threat. Make sure that playbooks identify all the integration points (contacts and procedures) that align IR to other business functions. For example, IR processes will hand off the technical response function to IT groups when it is time to "recover." Provide detailed guidance and decision trees in the playbooks on how and when to communicate with law enforcement, the media, and other third parties. Use NIST 800-61[8] Appendices A.1 and A.2 as starting points; the Appendices provide a list of questions to leverage for playbooks on multiple types of incidents.

9.6 Recover from Incidents Caused by Cyberattacks and Operational Outages

Recovery is different for incidents caused by cyberattacks than for those caused by IT system outages. In the case of a breach from a cyberattack, the technical security response team takes the lead during the IR recovery phase and may later hand off to IT or business continuity teams to lead recovery. In the case of an outage, IT and business continuity teams handle the recovery, and security operations may not need to be involved. Figure 9-6 depicts the high-level sequence of response through recovery activities for breaches and/or outages.

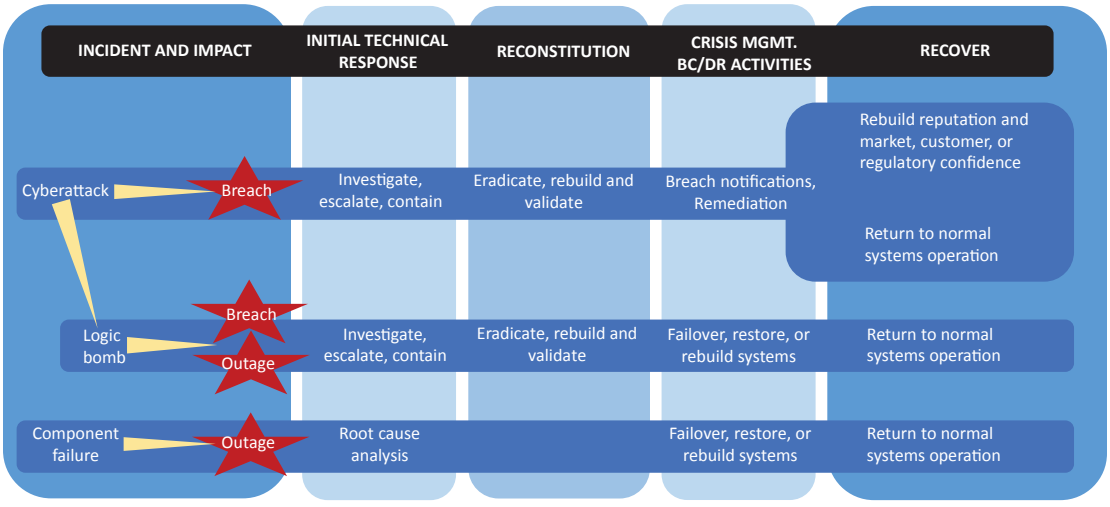

Figure 9-6. *Breach and/or Outage Response and Recovery*

Incident and impact:

- **Cyberattack scenario:** Figure 9-6 depicts a breach – such as theft of personal or confidential information. Once it is discovered, staff should perform an investigation to assess the impact of the breach and deny the attacker reentry, but in this case may not need to take down production systems.
- **Logic bomb scenario:** Suppose the same malicious actor causing the breach also left a logic bomb that damages production systems. This incident requires the IR team to lead a response, but because it also causes an outage, BC/DR plans should be activated.
- **Component failure scenario:** Figure 9-6 also depicts an operational outage due to a component failure, which could have been caused by human operator error, hardware failure, or some aberrant interaction of software and services. No malicious actor is suspected.

Initial technical response: For all breaches and outages, it's important to pinpoint the threat event. Why has the incident occurred, is it over, or is it just beginning? In the event of a cyber-incident, expect the worst from the malicious actor. Contain the cyberattack from causing further damage. Escalate notifications, support requests, or decisions to business functions such as legal, HR, IT, development, and executive management as required.

Reconstitution: Only after initial technical response and investigation completes can the IR functions fully reconstitute affected systems or applications by eradicating cyberattack artifacts such as malware, backdoors, compromised accounts, and so on. In some cases, systems are down and must be rebuilt to recover from an outage due to a cyberattack. In other cases, systems don't go down but some must be taken offline and surgically rebuilt to ensure no trace of malware remains. When rebuilding systems in this way, be sure to perform thorough scans and take other measures to validate they are clean. Reconstitution involves returning systems to fully operational states. It reflects mission and business priorities and may be driven by recovery point/time objectives and other metrics.

Crisis management, BC/DR activities: Any major breach of confidential information can provoke a crisis. In the case of an identity data breach, the IR team must coordinate notification of authorities, partners, the affected persons, and the media.

In the case of a breach of trade secrets, the business must notify partners where contractually required, and may have to scramble to contain further legal and market impacts.

Treat crisis management as the tactical problem that it is. The sequence of steps required to investigate and remediate the breach, notify interested parties, or make restitution vary with the type of breach. Response plans rarely cover 100% of the actions needed during a crisis but should lay down guidelines, requirements, and responsibilities to facilitate and speed decision making.

Recovery: Although business systems such as ecommerce sites may never actually shut down during the breach and the recovery goal is usually to continue normal operation, few businesses emerge from a breach unscathed. Post-breach businesses may move into a "new normal" of partner dissatisfaction or regulatory scrutiny that requires short-term changes to pricing, business practices, and supporting technologies. Over the long term, the business must work to rebuild damaged reputation, market share, and regulatory confidence.

9.6.1 Activate Business Continuity and Disaster Recovery Plans

BC/DR activities: In the event of an operational outage, BC/DR plans kick in. These plans should call for a root cause analysis, though this may be a quick process for outages that are due to a known and expected failure mode. Based on the BC/DR plans, determine the best course of action to restore normal operation: Failover has the least impact and may be possible for known incidents to critical systems with a hot standby capability. Restoring or rebuilding systems has more impact but continues to be an IT or development-led project.

9.7 Call to Action

The core recommendations for security leaders from this chapter are to develop cyber-resilience as follows:

- Identify critical assets through a BIA and create a BC/DR plan.
- Identify top risk scenarios through enterprise risk assessment and document risk appetites.

- Identify contingency plans for response and recovery.
- Identify strategic decisions (or phasing) for use of MSSPs, cyber-insurance, breach response services, and 24x7 SOC.
- Create detection capability by
  - Standardizing basic logging, log collection, and log review across IT environments
  - Developing basic automated event and alert monitoring
  - Engaging knowledgeable business and external stakeholders to understand and help monitor for threats
  - Advancing security analytics, detection engineering, and proactive threat hunting (required for organizations under high security pressure)
- Prepare response capability by
  - Designating a dedicated CSIRT role or forming a team; coordinating response plans with business executives, legal, HR, TPRM, public relations, and so on
  - Developing playbooks and procedures for technical response, investigation, escalation, and stakeholder notification during a breach
  - Ensuring response (and recovery) plans include a lessons learned phase in which gaps can be identified and procedures updated
- Lay the groundwork for recovery by
  - Planning separate but overlapping processes for responding to cyberattacks and operational outages
  - Ensuring that senior business stakeholders support the business continuity program and that the key IT team members who work "hands on" with mission-critical services are engaged

Action – Make a quick assessment of the organization's cyber-resilience

Ask yourself the following short set of questions and score the answers in the Success Plan Worksheet's[12] Section 3, Table 3. Base your score on whether you would answer most of the questions with a strong "no" (1), a strong "yes" (5), or something in between.

1. Does the business have
   a. Log standards?
   b. A security operations center (SOC) and/or an MSSP?
   c. A security information and event management system (SIEM)?
   d. A Computer Security Incident Response Team (CSIRT)?
2. Does the business have incident response plans and playbooks?
   a. Have these plans and playbooks been proven effective in real incidents or tests?
3. Does the business have an asset inventory and a current business impact assessment (BIA) identifying critical assets?
4. Does the business have a business continuity and disaster recovery (BC/DR) plan and program?
5. Has the BC/DR plan been tested?

Action – Define 1–3 improvement objectives for cyber-resilience

Note improvement objectives in Section 4, Table 10, of the worksheet. The following are some sample improvement objectives.

- Review contingency plans for incident response for the business's top risk scenarios or critical assets. Identify and list which are missing. If none are complete, develop a detailed outline for at least one plan and discuss it with affected stakeholders.
- Review incident response policies and procedures with affected stakeholders to ensure they are up to date and still agreed on.
- Review BC/DR plans with affected stakeholders to ensure they are up to date and still agreed on.

[12]"Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet