WHITE PAPER

THE NEED FOR EFFECTIVE INCIDENT RESPONSE

A cybersecurity breach is nearly inevitable, so organizations must be prepared to respond.

EXECUTIVE SUMMARY

Cybersecurity is a pressing concern for virtually every organization in today's digital world. From simplistic phishing attacks to malware developed by sophisticated nation-state actors, organizations face an unprecedented array of threats and growing concern over the potential impact a security incident might have on their operations. Leaders see other firms suffer from reputational damage after breaches of personally identifiable information involving their customers and employees. Managers watch other firms crippled by ransomware struggle to restore operations.

Building a strong, capable cybersecurity incident response program creates resilience against these threats. An organization that quickly detects security incidents as they occur can move rapidly to contain and eradicate the threat and return to normal operations more quickly.

As they move to establish an effective incident response program, organizations should start by addressing three critical questions:

- **Why has incident response become a key element of cybersecurity?**
- **What solutions and services are essential for incident response?**
- **What are the key elements of an effective incident response strategy?**

The answers to these questions should form the basis of a robust incident response capability composed of trained staff, effective technology and responsive service providers.

What Is Incident Response?

Modern organizations face unprecedented threats to the confidentiality, integrity and availability of their critical information assets and data. In previous years, the mindset of many cybersecurity professionals and business leaders was focused on avoiding attacks and building a strong perimeter to deflect them. However, more recently this approach has shifted, and these leaders now understand that attacks are inevitable. With this fundamental shift in thinking, cybersecurity professionals must build strong incident response programs that are capable of detecting threats in a timely manner and responding effectively when they occur.

Approaches to incident response may vary by organization, but at its core, incident response is a structured and coordinated approach to handling security breaches. This response occurs with the aim of moving as quickly and efficiently as possible from the initial detection of an incident to final resolution. Strong, well-coordinated incident response efforts achieve this with as little impact on business operations as possible, allowing the organization to balance business requirements with cybersecurity objectives.

The World Has Changed

Dramatic changes in the cybersecurity threat landscape began to alter the philosophy of cybersecurity professionals in recent years. While they once had the goal of building impenetrable defenses to keep attackers at bay, the greater sophistication of adversaries and the increased complexity of operating environments have rendered this approach virtually impossible. Organizations are left with one overarching security problem: There is simply no way to guarantee that they will be able to keep cybercriminals from establishing a foothold within their organization's technology environment. The threat is real, and the risk of compromise is no longer a matter of if, but when.

This new environment is the result of a combination of factors coming together at the same time. First, cybersecurity threat actors have become far more sophisticated. Nation-states and cybercriminals now leverage vast networks of attackers with advanced capabilities. These capabilities allow attackers to penetrate virtually any target, given enough time and patience. Second, these actors are targeting a broad range of interests. While advanced persistent threats once focused exclusively on high-value government targets, their reach now extends to businesses and nonprofits with information or resources that might advance the attacker's interests. As a result, organizations of all sizes are paying significantly more attention to cybersecurity. A robust security program is no longer a "nice to have" item but a strategic imperative.

The percentage of security incidents that involve internal actors[1]

From Perimeter Defense to Defense in Depth

At the same time that the threat environment changed, the technology environments of every organization across all industries became more complex. In the old model of computing, employees traveled to work in a central office every day and used the computers sitting on their desks to access servers maintained in the data center located in the building's basement. In today's business environment, users are spread around the world and need to access information at all times of the day and night from both corporate and personal devices. That data is no longer contained in a single data center but spread across multiple data centers and cloud service providers.

Source: [1]Verizon, "2020 Data Breach Investigations Report," May 2020

Defending the network of yesterday was a fairly straightforward task. Network security professionals built a strong perimeter around an organization's physical facilities and focused their efforts on keeping unauthorized people from accessing internal resources. Today, this perimeter approach has become ineffective. There are simply far too many endpoints distributed in far too many locations to make it practical to build this type of monolithic defense. When attackers have many potential targets, they can simply turn their attention to the weakest link in the chain to establish a foothold in an organization. Why attack a well-defended perimeter when they can simply launch a phishing attack against an administrative assistant instead?

The defense-in-depth approach to cybersecurity addresses this issue. Instead of relying on a few monolithic security controls, organizations build a set of overlapping controls designed to achieve the same objective. If one control fails, the others can pick up the slack. While it might not be possible to prevent all attacks from succeeding, the defense-in-depth approach makes the attacker's job harder and provides defenders with more time to potentially detect and deflect an attack. Minimizing dwell time, the time that an attacker remains on a network undetected, becomes crucial because the longer the dwell time, the more damage an attacker can do. A 2020 report from FireEye determined that the median global dwell time fell from 78 days in 2018 to 56 days in 2019. Among the factors the report identified as contributing to this decline were "the vigilance of security staff and investments in advanced technology and managed detection and response (MDR) services."

In the end, it all comes down to preparedness. Organizations that think about incident response in advance find themselves much better positioned to react when an incident occurs. They have asset tracking and other security controls in place that provide visibility into their operating environments. They understand their priorities and can quickly determine what data and systems are essential as they work to restore operations after a security incident.

The stark reality is that many organizations have not tested their incident detection and response capabilities. They don't know what tools they have at their disposal or how to use them properly during an incident response effort. This slows down response activities in an environment where quick detection and response are critical to protecting data. Attackers who are skilled and organized can take advantage of unprepared targets and extend their dwell time, allowing them to steal money, intellectual property and sensitive information.

Working Under the Presumption of Compromise

In years past, cybersecurity teams operated under the assumption that they could build strong defenses that would keep attackers out of their environments. However, attackers have grown more sophisticated and well resourced, while operating environments have grown more complex. This combination of factors makes it increasingly difficult to depend on a strong layer of defense to prevent all possible attacks.

The new mindset that many security professionals have adopted is known as the "presumption of compromise." In this approach, cybersecurity analysts assume that attackers will inevitably penetrate their defenses and gain a foothold in their organization. After all, it is quite difficult for most organizations to defend themselves against a determined nation-state attacker.

Working under the presumption of compromise changes how cybersecurity professionals think about all stages of their work. Design efforts focus not only on building strong perimeters but also on segmenting internal systems and isolating valuable data assets, limiting the spread of an attack. Ongoing analysis shifts from one focused solely on intrusion detection and prevention to a broader focus that includes threat-hunting efforts designed to ferret out existing compromises.

Elements of Incident Response

Effective incident response strategies require a strong foundation of security solutions and services that enable the collection of data and implementation of appropriate response efforts. Organizations with a robust cybersecurity program will find themselves well positioned to conduct effective response efforts in the event of a security incident.

Security Solutions Enable Incident Response

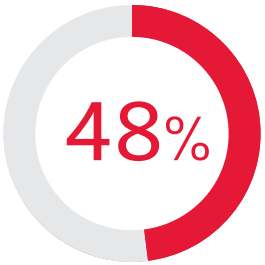
Threat intelligence solutions form the core of an effective incident response program. The cybersecurity threat landscape is constantly evolving and requires constant attention as new adversarial tools, tactics and procedures emerge. **Threat intelligence** solutions provide cybersecurity teams with actionable intelligence that they can use to bolster their defenses and recognize attacks from sophisticated adversaries. Threat intelligence products come in two forms: subjective assessment reports that inform cybersecurity professionals of emerging threats and technical feeds that allow the real-time incorporation of threat intelligence data into other security tools.

Endpoint security also plays a crucial role in detecting and responding to security incidents. Modern **endpoint detection and response** solutions go far beyond the signature-based capabilities of anti-malware packages to provide security teams with deep visibility and logging of all activity that takes place on an endpoint. EDR solutions not only help identify intrusions as they happen but also create a valuable audit trail that incident responders can reference as they attempt to reconstruct the actions of a successful attacker. Effective cybersecurity programs also incorporate server-centric solutions, such as email security packages that can watch for inbound threats, blocking them before they reach user inboxes.

These security products produce massive amounts of information, and the flows of data from all elements of a security

infrastructure will quickly overwhelm even the most diligent analyst. That's where **security information and event management** solutions come into play. SIEM solutions collect event data from all of these devices and aggregate them on a single platform, where incident responders can correlate events across systems to get a full picture of an unfolding incident. They may also take advantage of advanced **security orchestration, automation and response** platforms to initiate automated workflows in response to significant security events. Many of these SOAR platforms also incorporate **artificial intelligence and machine learning** to reduce the burden on human analysts.

Network segmentation plays an important role in containing the damage from a security incident. Unlike the flat networks used years ago, organizations now segment their networks as much as possible, grouping systems of similar security levels together. This approach prevents an attacker who compromises a system on one segment from using that compromise to pivot the attack to systems on other network segments, reducing the potential scope of the compromise. **Microsegmentation** takes this approach to an even greater extreme by separating individual workloads onto their own virtual network segment. The microsegmentation approach dramatically reduces an attacker's ability to traverse the network, but it also adds complexity for network security administrators who must manage the controls that enforce microsegmentation and allow communication between segmented systems.



The percentage of organizations that say they lack the budget to obtain the tools and technologies needed to support incident response[2]

Recovery efforts are also an important part of incident response. The stark reality is that some security incidents damage both information and systems, requiring that incident response teams turn to their disaster recovery plans to get an organization back up and running again. An incident response effort is not over until those recovery efforts are complete. Organizations that have a robust backup strategy will find themselves well positioned to conduct post-incident recovery efforts. Far too many organizations have discovered that their backup strategies were ineffective only *after* a debilitating ransomware attack. Conducting regular backups and storing them offsite increase the likelihood that an organization can quickly and effectively recover operations after a serious security incident.

Incorporating Machine Learning into Cybersecurity Efforts

It's hard to find a cybersecurity solution today that doesn't hype its machine learning and artificial intelligence capabilities. Organizations are rapidly adopting these business analytics techniques. But what exactly are these tools, and how do they play a role in cybersecurity work?

Artificial intelligence is a broad field that brings together the tools of computer science, statistics and mathematics in an attempt to replicate human thinking patterns in technology. Machine learning is a subset of artificial intelligence consisting of techniques designed to allow machines to learn by studying a data set. In cybersecurity applications, the terms are often incorrectly used interchangeably.

Cybersecurity applications of machine learning are incredibly promising, and vendors are incorporating machine learning capabilities into many security platforms. For example, a SIEM tool can use machine learning to easily identify abnormal patterns of user behavior. A next-generation firewall can detect and block suspicious traffic without human intervention. Intrusion prevention systems can piece together attack patterns on networks based on threat intelligence.

IT leaders should watch for ways to take advantage of machine learning capabilities in their existing cybersecurity tools and consider including evaluation of these capabilities in vendor assessments.

Services Supplement Internal Teams

Organizations need more than just technology to establish an effective incident response program. They also need talented staff with the skills and expertise necessary to detect, investigate and respond to a variety of cybersecurity incidents. Unfortunately, there is a serious skills shortage in this field, and organizations find themselves looking for talent in a highly competitive market. Fortunately, service providers such as CDW offer incident response expertise that organizations may use to supplement the resources available through their in-house security teams.

From a strategic perspective, CDW's incident response professionals can help ensure that business and technical leaders are prepared to respond to any type of security incident that arises down the road. This includes conducting incident response planning workshops and tabletop exercises that get an entire team on the same page while familiarizing team members with industry-standard best practices in incident response. When an incident strikes, teams must be ready to act quickly, and a solid plan provides them with the confidence to do so.

As an organization fleshes out its incident response program, third-party partners may also offer more technical exercises designed to help first responders and other technologists understand the processes of incident response. This includes blue team exercises, where the team works to defend an

Source: [2]SANS Institute, "SANS 2019 Incident Response (IR) Survey: It's Time for a Change," July 2019

organization against an unknown threat; and red team engagements, where exercise participants go on the offensive against their own organization to better understand its security posture. Purple teaming exercises combine red and blue team efforts, conducting defensive and offensive operations at the same time, allowing the organization to validate its defenses and identify security gaps.

Other services, such as CDW's compromise assessment program, recognize the new world of cybersecurity and the presumption of compromise by bringing threat-hunting services to organizations. In these engagements, security consultants use their incident response expertise to hunt for indicators of compromise on the client network and ferret out compromises that may be lying dormant.

Finally, a partner can assist an organization in the event of a security incident through on-demand incident response services. These engagements generally involve trained incident response experts who are ready to assist within minutes.

Strategy for Incident Response

Organizations that succeed at incident response generally rely on a formalized and documented incident response strategy. This strategy should be developed with input from IT leaders, executive leadership, functional line of business leaders and subject matter experts from across the organization. Incident response efforts involve cybersecurity teams, business leaders, attorneys, public relations teams and others, so strategic planning should also include those stakeholders. The plan they develop must address known vulnerabilities and also consider the need to uncover unknown vulnerabilities in the future.

Prepare for Incident Response

As organizations prepare for incident response, they should develop an inventory of their security controls and understand their own capabilities for incident response. The preparation phase should include establishing communication protocols and incident-handling playbooks that the organization will follow when an incident occurs. First responders should know how to activate the organization's incident response capabilities quickly and pull together the experts who will conduct most of the response. The strategy must spell out individual responsibilities and lines of communication during an incident, and each person must clearly understand his or her role. Responders must also have access to system and application inventories and documentation to help them zero in on affected resources.

Perform a Gap Analysis

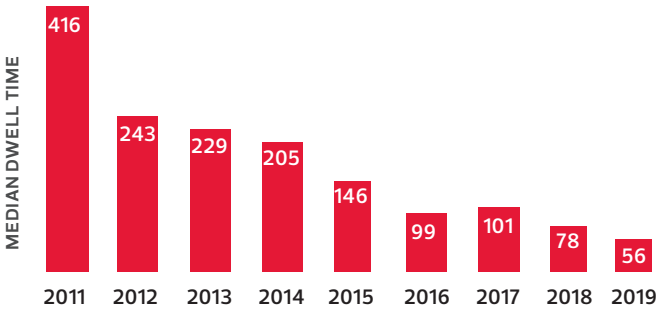
After developing an incident response strategy, an organization should conduct a gap analysis to identify flaws in its approach that require remediation. It's far better to discover a flaw before an incident, when the organization has time to remediate it, than to wait until disaster strikes to realize that the security controls in use are not adequate to support the incident response effort. The gap analysis should include a prioritized remediation plan that will serve as a blueprint for improving the organization's security posture.

Monitor and Automate

It's impossible to understate the importance of strong monitoring in any incident response strategy. An organization's SIEM platform is the focal point of many cybersecurity efforts, including incident response. Without quick and complete

Significant Decline in Dwell Time

Over the past nine years, FireEye has observed a major decline in the median number of days an attacker is present in a breached network before being detected.[3]



Introducing Purple Teaming

Cybersecurity exercise participants are traditionally organized into teams named after colors to provide a shorthand notation for their exercise roles. Borrowing this terminology from military exercises, the blue team consists of "friendly" forces who are responsible for defending assets against attack. The red team plays the role of the adversary, seeking to defeat the defenses erected by the blue team. A white team of neutral moderators facilitates the exercise, handling rule disputes and providing the scenario.

Recently, cybersecurity teams began introducing the concept of purple teaming into their exercises. Purple team exercises begin with the normal red team and blue team activities. As the exercise unwinds, the facilitators gather together the red and blue teams for a walk-through session where each team explains how the exercise unfolded from its perspective.

The purpose of a purple team session is to put all of the cards on the table and let the members of each team learn from the other team's perspective. The blue team gains deep insight into how the red team went about its attacks, while the red team gets an inside look at the response efforts. Running a purple team exercise enhances the learning experience for all participants.

Source: [3]FireEye, "FireEye Mandiant M-Trends 2020 Report," February 2020

access to information, incident responders are flying blind. Cybersecurity teams should continually ensure that the SIEM tool is operating effectively and that it is receiving information from all relevant sources in the organization. This becomes a complex task in a rapidly changing technology environment, as new systems must be connected to the SIEM as they are installed, and the SIEM must be properly configured to interpret and correlate data feeds from these new sources.

Automation plays a crucial role as an enabler of incident response. Organizations that go beyond simple SIEM deployments and incorporate security orchestration in their workflows will reap tremendous benefits in their incident response programs. In some cases, automation platforms will be able to respond to an incident and conduct a full recovery without human intervention. In other cases, automation will rapidly pull together the information required by a human analyst, reducing response time and improving the organization's ability to quickly contain an incident before it spreads.

You Play Like You Practice

Incident response is a learned discipline that depends on rapid action by knowledgeable people. Fortunately, many organizations don't need to activate their incident response programs frequently. While this is, of course, a good thing, it also means that incident response skills can get rusty, threatening the ability of responders to handle future incidents. CDW recommends that organizations conduct incident response testing annually to keep skills sharp.

CDW: We Get Incident Response

CDW is your organization's enhanced incident response partner. Our team of engineers, architects and consultants have decades of expertise in cybersecurity and can help you optimize your incident response strategy.

CDW helps organizations find the right cybersecurity solutions and services to meet their needs and provide the basis for a robust incident response program. Our team will work closely with you to determine your security needs and develop a range of options that fulfill those requirements while fitting within the constraints of your organization's budget.

Our incident response services team can assist you in all phases of your incident response effort. We're available to conduct incident response planning workshops and exercises, including purple teaming efforts. Our incident response team is also available to assist you in the event of an incident through our CDW compromise assessment service. Our team routinely enters into no-fee retainer agreements that make our services immediately available to you in the event of an emergency. Clients can call CDW's 24-hour security operations center, and CDW will have trained incident response experts ready to assist within minutes. If your security team is short-staffed, we offer a fully managed SIEM monitoring service to help reduce the burden.

CDW AMPLIFIED™ Services

CDW Amplified™ Security services are composed of both information security and network security practices, offer an objective look at your current security posture and provide continuous defense against, detection of and response to growing threats.

DESIGN for the Future
All CDW Amplified™ Security services provide a comprehensive approach to prevent data breaches and proactively respond to cyberattacks.

ORCHESTRATE Progress
CDW Amplified™ Security engineers can assist with installation and deployment of advanced security techniques and ensure technologies are optimized for your needs.

MANAGE Operations
We can manage security solutions for you, helping you stay vigilant and maintain compliance while easing the burden on your IT staff.

Sponsors

vmware Carbon Black CROWDSTRIKE MANDIANT

To learn more about CDW's incident response services and solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/security.

CDW PEOPLE WHO GET IT®