Secureworks®

WHITE PAPER

You've Been Compromised: Now What?

Staying in Control When an Attacker Strikes

Chaos seems to reign when a fire station responds to an emergency, but the blaring alarms and rotating lights obscure what is a high functioning operation. Extensive preparation and planning mean every member of the station knows the job they must perform.

Smart cybersecurity operations function in the same way. When an attacker strikes, a security team has detailed plans and procedures to follow to speed response and remediation. At the best prepared organizations, little is left to chance.

Constant tabletop exercises and simulation scenarios help validate what works in a plan and highlight what doesn't. This encourages speed and certainty under pressure. Without a plan, organizations run the risk of poorly coordinated incident response (IR) activities that could cause more damage than the compromise itself. Responding to a cyberattack is the worst time to discover that you're unprepared.

Without a plan, organizations run the risk of poorly coordinated incident response (IR) activities that could cause more damage than the compromise itself.

What's it Like During an Incident?

Many companies experience a range of emotions, from shock, to bewilderment, anger, and frustration. On the IT side, there is the potential for chaos as different teams and cross-functional groups inside and outside the organization are looking for answers — and sometimes someone to blame.

Working across the organization, the incident response team needs both technical expertise and political savvy as they navigate heated situations where tempers can flare. In these situations, it's important everyone within the organization looks after their emotional well-being. Answers to questions are rarely available immediately. Days, weeks, or months can pass before the investigation is finished.

Senior leaders should understand the investigation and fact-finding process takes time and can vary significantly depending on the nature of the attack. Because of this uncertainty, it's important to notify business leaders as soon as possible when new information arises.

What's the Mindset Like Inside an Organization?

After a cyber incident, there's always a degree of chaos and unrest within an organization. Management, in partnership with the legal department, can help set an assured tone that will filter down through the business.

Despite what may be happening behind the scenes, the reaction from the top should be measured and reassuring for the rest of the company. Leadership should also consider the sensitivity of holding individuals or teams accountable for an incident.

Half of the battle rests in the IR team knowing their assignments and understanding who is leading the investigation. Leaders across the business from C-level, to directors, to managers, must have faith in the team members that have been assigned to execute the response plan. This is where organizational involvement, training, cyber education, and tabletop exercises are critical to how an organization responds.

Whether a compromise is suspected or confirmed, the organization's Cybersecurity Incident Response Plan (CIRP) should be activated.

How Should an Organization Respond?

Every cyberattack is different. Some are easily detected or quickly contained while others may emerge over time. Whether a compromise is suspected or confirmed, the organization's Cybersecurity Incident Response Plan (CIRP) should be activated.

The first 24 hours after an attacker gets in are critical. Unfortunately for some organizations, issues aren't escalated in a timely manner, meaning incidents can stagnate and increase the risk of damage. Once your response plan is activated and live, this is how events usually unfold:

The incident response team is convened. The IR plan contains a list of cross-functional teams, information security people, and C-level executives who are notified along with key personnel that are tasked to perform a function.

A designated authority figure guides the process. This could be an incident manager, who focuses on the technical aspects, or an incident owner who works with the lead investigator, documentation and timeline lead, communications lead, and any legal and HR representatives. Most plans call for both roles, as they usually work in tandem and assess damages. One of these figures is assigned ultimate authority.

Members of the incident response team help protect any intellectual property or customer data and oversee compliance with data security regulations. Leaders should help guide response, escalate actions, and have confidence in their security organization, but should resist the temptation to help with tactical elements of the response.

Assigned IT and security teams remove or isolate the threat. They analyze and interpret logs, determine the cause and extent of the damages, and help lead forensic evaluations. IT and security may coordinate any recovery efforts as well as preserve any evidence.

In-house legal counsel and compliance officers identify who they need to notify of the incident, including outside counsel, and navigate privacy laws, federal and industry regulations. There may be contractual requirements that could come into consideration after systems or data are compromised. Legal teams must also assess the possibility of applicable fines the company may need to pay and foreseeable litigation from affected parties.

IT attempts to determine the root cause of the incident. If you contract a third-party vendor for response help, they will work with your IT team, management and sometimes your legal team to conduct an investigation into the nature and extent of the compromise. Understanding what happened will be instrumental in helping to contain the damage.

Public relations and marketing will draft press release statements and the internal communications team usually finds the best way to communicate the events to employees. They team up with members of senior leadership to craft the right messaging for the company's pre-assigned spokesperson. PR and marketing, working closely with legal, are responsible for contacting the media, announcing to the public and internal communications. They also monitor and assess potential public reaction in response to a security incident. They're also instrumental in developing the post-incident messaging or any boilerplate statements for media.

Business units work to define critical business impact and maintain business continuity.

Any additional third-party vendors should help with incident response and forensics. This can lead to significant delays depending on the IT and security protocols of the vendor. They will also work with management on any legal, regulatory, and service issues. If your organization has cyber insurance, this introduces another layer of people for your team to coordinate with.

Post-Crisis and Lessons Learned

Once an incident is contained and business operations are restored, organizations should hold a postmortem meeting to assess the effectiveness of their response. This should include incident response team members and your third-party service vendor. Identify in your plan which department or employees should lead the post-incident assessment.

Any knowledge gained from threat analysis will be used to help the organization prevent any future cyberattacks. Consequently, any data, trends, patterns, observations, or pertinent information that comes from these meetings can be used to build the next phase of incident response planning. In some circumstances, organizations don't act on all the residual risk which needs addressing, often due to time and resources. Somebody should be responsible for signing off on these decisions.

Postmortem meetings are designed to help the incident response team and organization better understand what worked and what didn't work during the response effort.

These meetings can reveal valuable information such as:

- Why the incident happened.
- Whether subsets of issues contributed to the attack, such as weak passwords, or the bad actors used multiple attack vectors to achieve their objective.
- Other vulnerabilities in your security controls.
- The outstanding risks that can be remediated.
- Whether the incident was caused by human error or tool misconfiguration.
- Whether you're missing the right skill sets on your team, or your team members are overworked and burned out.

Your lessons learned meetings can play a critical role in determining whether the organization will suffer in terms of operational integrity, reputation, or legal liability. It can also expose excessive bureaucratic layers that may have led to a delayed response, as well as gaps in staff training and loopholes in the systems that were exploited.

Improving Incident Response with a Vendor

Post-incident, many organizations realize response could've been improved with the expertise of a security partner. Sometimes, if a security vendor was called in to guide the response, the incident postmortem might suggest the response wasn't as good as it could've been. Unfortunately, on occasion the mistakes an IR vendor makes aren't identified, and there is still the risk an issue could be lurking somewhere undetected.

Many security companies offer incident response services, but results vary widely depending on the provider. Like other areas of security, the IR marketplace is crowded and confusing. Complicating this situation is the fact some vendors don't have the knowledge or tools to identify all the issues and successfully mitigate risk. A seemingly "successful" response can conceal hidden problems.

Comprehensive incident response requires a vendor that has expertise in three critical areas:

Threat Intelligence: Detailed, proprietary global threat intelligence compiled by world-class researchers enables a vendor to identify more threats, know what to look for, and determine knock-on impacts for other areas of an organization. Great threat intelligence allows a vendor to look beyond the threats hiding in plain sight.

Breadth of Industry Experience: Every company's security environment, industry and organizational characteristics are different. A vendor with a long history serving thousands of customers across all industries, is better placed to navigate your environment and understand the implications across departments.

Powerful Analytics: Threat intelligence is the ability to identify threats and understand the hallmarks of threat actor behavior. Analytics allow a vendor to scale this knowledge and use it to analyze activity in any security environment to identify threats. As threat actors employ stealthy tactics to evade traditional defenses, it's critical a vendor can detect behavioral clues.

These three areas help a vendor respond effectively and thoroughly to an incident in your environment. They also equip a vendor with the necessary knowledge to help you build a robust Cybersecurity Incident Response Plan. Many organizations call in a vendor for the expertise needed to craft a CIRP. A vendor with a large, global customer base should have valuable insight into what works for companies of similar sizes and industries to yours. If they're also equipped with proprietary threat intelligence and a long history in the industry, a vendor will often identify areas of risk you may miss when drafting the CIRP internally.

Make Your Organization Cyber-Ready

Through the first quarter of 2020, a reported 8.4 billion records were exposed in data breaches.[1] In this climate, a robust Cybersecurity Incident Response Plan is imperative for any organization.

No single organization can match the expertise and depth of experience of the best security vendors, which is why many companies value the input of a security partner to drive and shape their CIRP. This benefit is compounded when the same vendor also provides incident support. Familiarity with the plan and your organization allows the vendor's IR team to work quickly and efficiently.

The CISO should ensure senior business leaders play a key role from day one of CIRP development and select the best vendor for both CIRP deployment and incident response support. The CISO should also encourage leadership to participate in tabletop exercises and ensure preparedness when an incident strikes.

If the success of a fire chief revolves around directing the activities of the fire department as well as being the sole authority and command at the scene of an emergency — then the success of a CISO is quantified by strong cross-organizational relationships, good cyber hygiene, proactive prevention measures, and organized responsiveness should an incident occur.

8.4B

Records were exposed in data breaches through the first quarter of 2020.[1]

[1] Risk Based Security, 2020 Q1 Data Breach QuickView Report

Secureworks®

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp