Secureworks®

WHITE PAPER

From Reactive to Proactive: Keys to Shifting Your Cybersecurity Strategy

Learn how to Prepare Your Organization
for Whatever the Future Brings

In 1907 Robert Baden-Powell conceived what would become the Boy Scouts of America motto, Be Prepared. Baden-Powell wrote that to be prepared means "you are always in a state of readiness in mind and body to do your duty."

Organizations should take note. A constant state of readiness is crucial when it comes to cybersecurity. Senior leaders who embrace this ethos stand a much better chance of minimizing the damages, risks, and costs than leaders who have no plan and respond to threats reactively.

At a minimum, practicing basic cyber hygiene can address or mitigate a vast majority of security breaches. Employee cybersecurity education can help your organization avoid phishing and spear phishing scams, provide a greater awareness of social engineering tactics, and help employees understand the different types of information that hackers seek.

Even with the best cyber awareness training, incidents happen. What then? For organizations without an incident response plan, a breach could spell disaster. That's why many organizations use incident response plans with detailed instructions to provide their teams with structure when trying to address a breach.

An IR plan is just one part of building a proactive approach to cybersecurity strategy, Creating an incident response plan doesn't guarantee a proactive posture, but it does reduce the risks of incidents for reactive organizations by providing concrete steps and structure to the response process. Organizations that rely on reactive measures alone, with no cybersecurity incident response plan in place, leave their organizations more vulnerable to chaos and potential disaster.

A constant state of readiness is crucial when it comes to cybersecurity. Senior leaders who embrace this ethos stand a much better chance of minimizing the damages, risks, and costs than leaders who have no plan and respond to threats reactively.

A Reactive Approach is an Effort in Futility

Reactive organizations only act once damage is done. This increases organizational risk and can amplify the negative effects of breach. Unfortunately, a reactive approach is the norm across cybersecurity departments. A recent Ponemon Institute study highlighted this fact.[1] They surveyed 577 IT and IT security practitioners in the U.S. and uncovered some surprising findings:

- 69% of respondents said their organization's security approach is reactive and incident driven.
- 63% of respondents said their IT security leadership needs better monitoring tools to help communicate security efficacy and gaps to the C-suite and board.
- 56% of respondents said their IT security infrastructure has gaps in coverage that allow attackers to penetrate its defenses.
- 40% of respondents said they do not quantify and track the company's IT security posture at all.

A reactive approach to incidents often ends in chaos. Why? Because new techniques are constantly employed, leaving an uncertain future when it comes to defending against threats.

A reactive approach is why many organizations take way too long to detect threats. On average, 206 days pass before a breach is identified and a further 73 days pass before a breach is remediated.[2] Imagine what a motivated threat actor could achieve in that time. A reactive strategy puts security teams at a huge disadvantage.

206

days pass before a breach is identified and a further 73 days pass before a breach is remediated.[2]

Shifting to a Proactive Cybersecurity Posture

A proactive approach to cybersecurity can put you on the front foot against attackers and keep you ahead of regulatory requirements. It helps your organization stay prepared and offers a concrete action plan. In the circumstances where your organization is reactive, it offers form and structure to avoid confusion. The goal is to avoid the elements of surprise and uncertainty which lead to a fumbled incident response. Here are some steps to help your organization transition from a reactive to a proactive security mindset:

[1] Ponemon Institute, The Cybersecurity Illusion: Enterprise Security Remains Reactive

[2] Ponemon Institute, Cost of a Data Breach Report 2019

1. Get Educated

The first step for business leaders is to understand what types of threats and risks your organization may face. Understanding what cybercriminals want and how attacks happen will help you identify the vulnerabilities of your infrastructure and processes. Older documentation offers an opportunity to evaluate processes and see what has changed within the organization — from new hardware, to software, to cloud migration. Useful documentation could include procedural guides, schematics, past playbooks, IT checklists, emergency contact numbers — this information can serve as a guide and a starting point.

Reviewing past documentation also allows you to identify themes and detect patterns like user knowledge (or lack thereof), or the company's attitude towards security practices and awareness. When considering awareness training, remember the importance of educating executives and employees in sensitive departments about spear phishing. But don't dwell too long on the past: cybercriminals are always evolving, and so should you.

2. Create an Incident Response Plan

An IR plan is a true investment in your business and one that involves the entire organization. A thorough plan designates key members of the incident response team, as well as individual roles and responsibilities, team structures, and escalation processes. An incident response plan should be truly cross-functional. Most plans involve significant input from each of these functions:

- General Counsel (Legal)
- Chief Information Security Officer or Chief Information Officer
- Technical Leads (such as Security, Network, or Infrastructure)
- Human Resources
- Public Relations/Marketing
- Risk Management/Insurance
- Business Subject Matter Experts (as needed)

It's common to have one single incident response team. Another option is to create a core team and bring on ad hoc members as each situation dictates. Either way, your plan should establish roles and responsibilities for when an incident occurs. This enables organizations to respond to a breach quickly and appropriately.

An IR plan is a true investment in your business and one that involves the entire organization. A thorough plan designates key members of the incident response team, as well as individual roles and responsibilities, team structures, and escalation processes.

For instance, if an insurance company confirmed that malicious code infected a core application, management could quickly decide to shut down all network access. Managers understand the risk of continued data loss from this action versus the associated loss of revenue resulting from downtime. There needs to be a designated person who has the authority to make these kinds of decisions. Equally, it's important that nobody possess a level of unchecked authority that allows them to make decisions that compromise the response and the organization's reputation.

Everyone on the incident response team must fully commit to the plan. Plans should be updated twice a year. To successfully implement the plan, it should be easily accessible in print, digital, and on an internal web-based platform. The goal is to make it as easy as possible to access, and to make sure everyone who needs it knows where it is.

An experienced vendor with deep threat intelligence will give you insight into the threat landscape that your security teams may struggle to get by themselves.

3. Communicate Value

When business leaders show they value cybersecurity it can have a large impact. This vision needs to be socialized across all levels of the organization. If you, and other leaders, show up when tabletop exercises are scheduled, it can send a powerful message to the staff that leadership is putting their money where their mouth is.

If you demonstrate an eagerness and deep commitment to protecting your company's digital assets, upholding trust, and making cybersecurity a business imperative, the rest of the organization will be inclined to uphold those values too.

On the contrary, if leadership pays lip service to cybersecurity by exhibiting poor cyber hygiene, their behavior will cascade down through the organization, exposing it to risk. Likewise, business unit leaders should amplify leadership's core cyber messages to their wider teams, so they understand the specific threats targeting their teams and the different roles they play in securing the organization.

4. Train Your Organization

Training is a great way to exercise your security muscle. Increasing awareness, promoting cyber education, and utilizing tabletop exercises can help encourage robust cybersecurity. Combine these with keeping up with the latest threats, and paying attention to other businesses within your industry, and you're ready to take the plan from a static document to being embedded in the fabric of the organization.

Selecting the Right Vendor

Partnering with a vendor that specializes in proactive cybersecurity practices can help you transition your strategy. For example, vulnerability assessments, penetration testing, threat hunting, and proactive incident response are all services that can help your organization shift from a reactive to a proactive stance. They can help you identify your security weaknesses, discover whether someone can break in and what they can get, and identify signs of an attack before one has occurred.

An experienced vendor with deep threat intelligence will give you insight into the threat landscape that your security teams may struggle to get by themselves. Vendors have a global view of threats, while your security team mostly only has visibility into what is happening within your environment.

Choose a vendor that has the context and perspective to truly understand your business and the goals of your cybersecurity program. A vendor with thousands of clients across the globe is more likely to offer rare context and insights than one that is small or focused on limited geographic areas or industries.

Remember to Be Prepared

Shifting to a proactive security strategy prepares you to meet any new trends, breaches, or intrusions that may come your way.

Organizations should consider how taking a proactive approach can ensure your organization's cybersecurity practices are sufficient and current enough to protect against sophisticated cyberattacks.

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