Secureworks®

WHITE PAPER

Meeting a Greater Demand for Cybersecurity

Empowering Security Practitioners to Achieve Success

It's no secret that cybersecurity is a hot topic among business leaders and board members – and for good reason. According to 2019 research from the FBI's Internet Crime Complaint Center (IC3), more than $3.5 billion was reported lost as the result of cybercrimes,[1] a devastating figure on its own, but the reality is compounded by the fact that cybercrime remains largely underreported.[2] Advanced threats are more prevalent, motives are more nefarious, and the perception that what's at risk doesn't impact the physical world has been repeatedly debunked by security professionals. Many executives now recognize the threat cybercrime poses to their business.

As a result, cybersecurity budgets have been increasing, with IDC projecting global security-related spend will reach $151.2 billion in 2023.[3] Yet security teams are not growing to keep pace with rising demands and expectations from leadership. Financial resources play a critical role in bolstering security defenses, but how those resources are spent is just as important. Although security has become an organizational priority, communication gaps between business leaders and security teams often trigger investments that aren't best suited to meet the needs of the organization or don't support the team's ability to defend against evolving online threats.

$3.5B+

was reported lost in 2019 as the result of cybercrimes.

$151.2B

in security-related costs will be spent in 2023 according to IDC projections.

Obstacles Overburdening Security Teams

Cybersecurity impacts business units across an organization, but outside of the security team, many see the security practitioner as a homogenous role charged with protecting the business from online threats. On its surface, that assumption seems innocuous enough, but it is a misconception that can directly obstruct a team's efficacy. Here's why. When decision makers – particularly those that control the budget – perceive security professionals as generalists, they risk investing in security resources that do not necessarily improve the organization's security posture.

Because security practitioners often specialize in certain industry domains, mapping organizational challenges to the necessary skills makes a big difference. Assuming security practitioners have a lot of overlapping skills oversimplifies the security landscape and often puts practitioners in the position of trying to do the job they were hired for while simultaneously trying to address gaps without the appropriate skills. Let's say a security manager tells her business leader she needs five skill sets to effectively deliver against the added demands for her team. If the organization can only afford three new hires, the security team may not be able to find the required skills across three experts, particularly in a competitive market where security vendors can often attract and retain the best talent.

[1] FBI Internet Crime Complaint Center, 2019 Internet Crime Report

[2] Information Systems Audit and Control Association (ISACA), State of Cybersecurity 2020

[3] International Data Corporation (IDC), New IDC Spending Guide Sees Solid Growth Ahead for Security Products and Services

Secureworks®

Misaligning skills and needs set up barriers to success from the beginning, but even with the right skills in-house, security teams are up against a constantly evolving adversary. The sheer volume of potential threats and tactics and how they can be deployed across different environments can dominate a team's time. On top of their day-to-day mandate, security professionals also must be prepared for how and when businesses deploy new technologies or acquire new businesses to protect, quickly determining if they have the right tools, skills, and support to adapt. Accounting for the time necessary to address emerging threats and newly identified vulnerabilities, it's clear why the increased demand is outpacing the rate at which in-house security teams can grow.

Know your limits. Most enterprises don't have to deal with the totality of security challenges, so investing in the infrastructure and expertise across every threat that could impact the business is inefficient and prohibitively expensive.

Security Technology Can Help, but There are Limits

When confronted with the challenges security teams face, decision makers often turn to security tools. C-suite leaders tend to favor tools because they cost less than people and can often be counted as assets. Security technology can help address an overburdened team, but it has limitations, particularly when the right skilled experts aren't present. Endpoint detection and response (EDR) and Next-Gen AV (NGAV) have been introduced and help, but they are no silver bullet. Many security tools now give too much information and lack context, making it difficult to prioritize what poses the biggest risk.

Additionally, most tools focus on prevention because it's easier to demonstrate the return on investment – which makes it more appealing to decision makers. That leaves huge gaps when it comes to detection, response, and prediction, and those vulnerabilities fall to security teams that aren't set up to succeed. Teams are experiencing information overload while trying to distinguish between real threats and false positives, a time-consuming undertaking that interferes with more meaningful work or addressing more persistent threats. While nation-state actors won't be targeting your organization every day, the problem is when they do select a target, advanced adversaries are sophisticated, well-funded experts that don't need to accept failure as an outcome. Protecting and defending against these attacks requires levels of expertise and context that would be cost-prohibitive to build internally when in-house security teams are still subject to business rules and must constantly justify expenses.

Addressing the Growing Demand Without Burning Out

The security marketplace is overcrowded; the range of technologies is immeasurable, and there are infinite ways a system can be configured. There is no standardized checklist that can be universally applied. Cybersecurity has changed, is changing, and will continue to change, but the knowledge gap between security practitioners and business leaders is contributing to wasteful investments, skyrocketing stress levels, and unrealistic expectations – one of the primary factors driving employee burnout.[4] Consider the following strategies to better equip security teams to address increasing demands in an ever-changing environment:

Enterprises need to support soft skills development for security teams. The better your team members communicate and work together, the more perspective they'll gain and the more effective and efficient they'll be.

If something isn't working, don't ignore it or make uninformed assumptions about the problem. Is there a mismatch between the environment and the skills? Is stress or anxiety overwhelming the team? Identify what kind of issue is impacting the effectiveness of your security response.

Practitioners must have the right tools and resources to work against the organization's unique environment. Throwing money or people at a problem without a deep understanding of how they map to the objectives limits the amount of success your team can have.

Know your limits. Most enterprises don't have to deal with the totality of security challenges, so investing in the infrastructure and expertise across every threat that could impact the business is inefficient and prohibitively expensive.

Security practitioners are specialists for a reason, and their skills are valuable in a complex, evolving, and relatively young industry. With demand on the rise, partnerships with security-focused vendors can provide your in-house team the breadth and depth of knowledge that would be extremely difficult to replicate and maintain internally. A security partner understands the threat, has experience across diverse environments and technologies, and can share expertise and perspectives that enable your team to work more effectively. If you find yourself overburdened by the increasing demands of today's cybersecurity landscape, it may be time to consider an external vendor that can support you and the needs of your team and business. The right partnership can help you prioritize the actions that yield meaningful, measurable outcomes and validate the capabilities and value security brings not only to IT but to the entire business.

The right partnership can help you prioritize the actions that yield meaningful, measurable outcomes and validate the capabilities and value security brings not only to IT but to the entire business.

[4] Deloitte, Workplace Burnout Study

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