Secureworks®

WHITE PAPER

10 Security Controls to Reduce Risk

It’s important for leadership in any organization to understand that optimizing your security controls is about more than just protecting data and systems, it’s about reducing your organizational risk as it aligns to brand, customer relationships, and overall operations.

Cyberattacks such as ransomware and business email compromise can have huge operational and financial impacts to an organization when they succeed. Cybercrime is predicted to cost the world $9.5 trillion USD in 2024[1], according to Cybersecurity Ventures. Even when they are mitigated, these attacks can cause serious disruption if they force you to take things offline to reset and rebuild. Some organizations can weather this kind of storm — others simply can’t, and they find themselves facing questions about the future of their organization they maybe never thought they’d face.

The Role of Security Controls in Maximizing Cyber Defenses

Security controls are your tools to reduce your risk and protect your organization from threats. Like risk, there is a lot of variety, but they all share the same goals of trying to prevent breaches from happening and reducing the impact on your organization when a breach does occur. Some are more fine-tuned in one area than the other, and many deliver different levels of impact across threat prevention, detection and response. Having the proper mix of strong security controls in all areas is a key part of establishing defense-in-depth.

Cybercrime is predicted to cost the world **$9.5 trillion USD** in 2024[1]

Strong security controls are also crucial to another way many organizations reduce their cyber risk— cyber insurance, which serves to transfer the costs of a breach. Expenses generally fall into two categories.

First-party liabilities are those you may incur directly as the result of an attack and/or breach. These liabilities can include the actual financial harm done to your organization, such as the cost of business interruption, theft, ransomware payments or the expenses involved in restoring affected data and IT systems.

[1] Boardroom Cybersecurity Report 2023, Cybersecurity Ventures

They can also include costs such as fees paid to breach consultants and cyber forensics firms, notifications to customers and other affected parties, and PR expenses incurred to reduce damage to your company's brand.

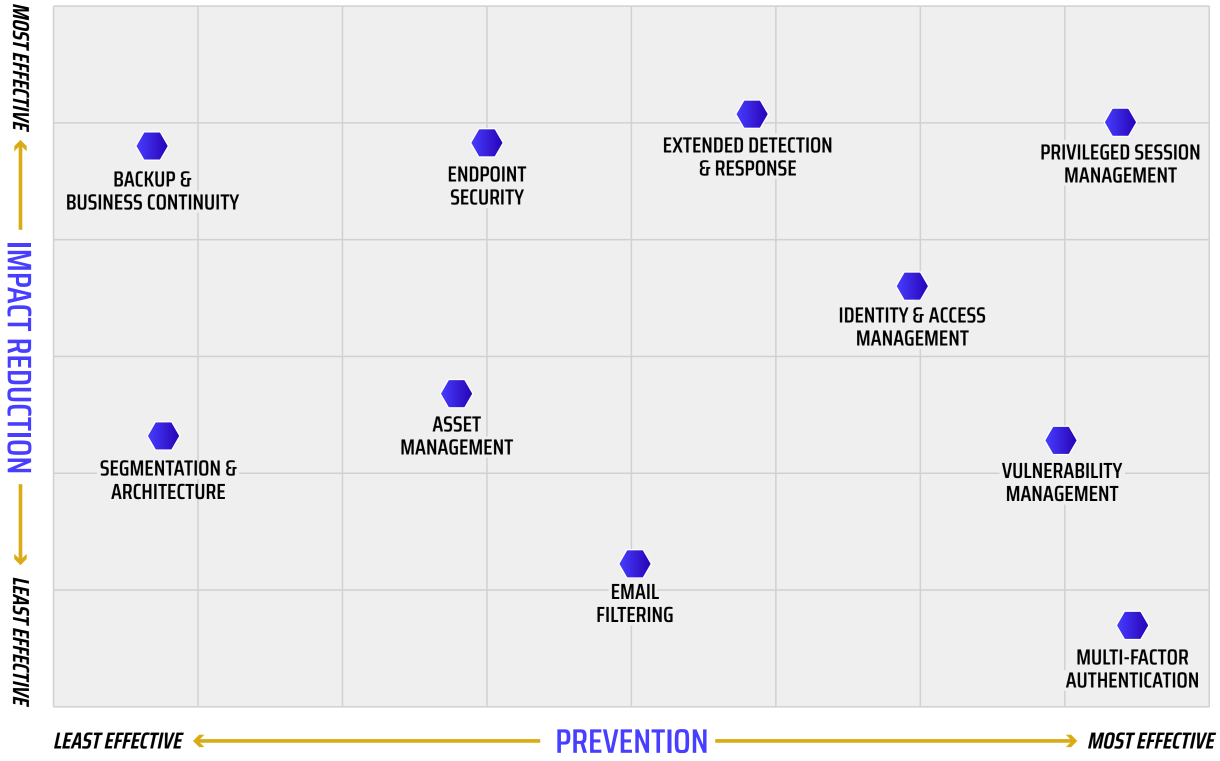
Third-party liabilities result from customers, supply-chain partners, regulators and others. They can include direct demands for compensation, lawsuits, and financial penalties imposed by government agencies and/or trade associations.

Cyber insurance premiums and coverage limits are based on a holistic review of a company's risk, and security controls play a major role in optimizing what kind of coverage is available to your organization.

Reduce Risk With These 10 Security Controls

Focusing on strong security controls will have the dual effect of both reducing your overall cybersecurity risk as an organization and helping you achieve the most cyber insurance coverage at the least cost, which lessens your financial risks. Looking at the spectrum of prevention and impact reduction, we've identified 10 security controls that have the potential to reduce risk at every organization, regardless of industry. Properly implemented, these 10 security controls can help create a cybersecurity posture that is ready to take on both the threats of today and those in the future.

10 SECURITY CONTROLS TO REDUCE RISK



Controls to Help Restrict Access

The first thing a threat actor must do is get into your system. These controls land high in preventing a breach from occurring in the first place.

1 Identity and Access Management

Identity and access management (IAM) ensures the right users have the appropriate access to technology resources. Many organizations will invest in Privileged Access Management (PAM) controls to minimize risk exposure, giving users the least amount of privileges needed to do their job. It may sound simple, but this can quickly become a quagmire in larger organizations. What systems are in place to grant and track access to software and systems? How are identities being removed when people leave the organization? Regardless of size, every organization should have strict rules around access and identity removal, otherwise those identities can quickly become a liability if a threat actor can compromise one.

As part of an IAM strategy, set policies for managing passwords and give people the tools to utilize best practices with their passwords. Pass phrases should be encouraged, and using multi-factor authentication along with biometrics can greatly improve the strength of your identity and access management, which in turn reduces risk.

Set policies for managing passwords and give people the tools to utilize best practices with their passwords

2 Endpoint Security

Protecting endpoints has seen increased importance as hybrid and remote working arrangements become more normalized. More devices on your network mean more entry points for threat actors. Reducing risk in this area is typically about having strong detection and response mechanisms in place. Threat actors will commonly deploy what's called "commodity" threats at endpoints, which are less sophisticated, low effort attacks used on a first attempt. These threats often have known signatures that make them easier to detect, so strong threat intelligence is critical to strong endpoint security.

One important thing to note with endpoint security is that every endpoint that is externally focused must be protected. Often an organization's weakest link is an old operating system or a new OT device that isn't supported by their current endpoint vendor. But you need to find a way. If not, you can bet that threat actors will find your weak points.

One important thing to note with endpoint security is that every endpoint that is externally focused must be protected

3 Multi-Factor Authentication

Multi-factor authentication, or MFA, is increasingly becoming normalized because of its strong ability to reduce risk when it comes to stolen credentials. At its most basic level, MFA is having multiple systems that will validate a person is who they say are when they try to log in. This is a critical component of your cybersecurity control environment considering that infostealer activity has increased[2], meaning that stolen credentials now rival scan-and-exploit as some of the most significant precursors to ransomware attacks.

As with all cybersecurity controls, best practices are continuously evolving with MFA. Many organizations are currently adopting an MFA requirement of having something that the person is (fingerprints or facial recognition, for example), something the person has (like a token) and something the person knows (a pass phrase or password).

Organizations also need to be aware that MFA is continually improving as threat actors learn to bypass more basic controls. More advanced methods such as geolocation and numerical matching may be needed to reduce risk. Geolocation technology can add another layer of identity verification by ensuring access attempts are made from familiar locations, minimizing the chances of unauthorized access. Additionally, numerical matching is emerging as an effective means of authentication wherein a sequence of numbers displayed on the user's device needs to be accurately inputted, thus making it challenging for attackers to bypass. As these advanced technologies are incorporated into MFA methods, organizations need to ensure the privacy and rights of their users are not compromised by the collection and use of geolocation data. Also, false positives could lead to unnecessary denials and inconvenience legitimate users, so mechanisms should be in place to minimize these. Finally, while these advanced methods should enhance security, they should not be so complex they impede workflow; they should offer robust security while maintaining user-friendliness.

More advanced methods such as geolocation and numerical matching may be needed to reduce risk

4 Vulnerability Management

Vulnerability management is a continuous process to identify potential weaknesses across your environment and ensure they are addressed. With common elements including software and system patching and configuration, strong threat intelligence can play a key role in ensuring you are up to date on identifying emerging threats.

[2] - 2023 State of the Threat: A Year in Review, Secureworks

Important aspects of a vulnerability management are understanding where all your assets are across your network and continuously and holistically scanning them, as well as taking a risk-based approach to prioritizing which assets are most susceptible to exploitation. When it comes to prioritizing, having full visibility into your security ecosystem is vital to prioritizing vulnerabilities based on the specific contexts of your organization and its environment.

Controls to Slow and Stop an Attack

When a breach does occur, these security controls can mean the difference between stopping an intruder and watching them take control.

5 Email Filtering

Email is often criticized for feeling antiquated and out of step with modern tech stacks, but it's still a critical function for many organizations, and it's still one of the top ways threat actors get access into your system. Threat actors send out thousands of phishing emails a day, and all it takes is one to cause huge problems in your organization. Business email compromise is one of the most frequent cyber insurance claims organizations make. It is also getting harder and harder to detect as threat actors leverage generative AI for better grammar and messaging. It's actually because of the longevity and ubiquity of email that these phishing attacks are so dangerous. Threat groups have had time to maintain and iterate on the malware those emails contain, so what is delivered is incredibly sophisticated and powerful. If it gets in your environment, it is going to test every one of your security controls across your architecture. Email filtering is an important preventative tool to reduce cyber risk, as the best way to fight a phishing attack is to make sure the recipient never sees it.

Business email compromise is one of the most frequent cyber insurance claims organizations make. It is also getting harder and harder to detect as threat actors leverage ge

6 Privileged Session Management

Related closely to identity and access management, privileged session management is all about protecting admin privileges in your environment. Compromising the identity of an every-day user will only get a threat actor so far in the system; however, if they want to do more malicious things such as disable endpoint detection, antivirus software, or deploy ransomware at scale, they need to acquire administrative-level privileges.

Reducing risk in this area requires a tiered model for administrative privileges where your highest level of privileges are the accounts that can control identity and access management. Keeping a threat actor away from administrative-level privileges is one of the most critical elements to get right in your cybersecurity strategy because if they are able to set themselves up as an admin, they can wreak havoc on a system-wide scale, deploying ransomware and removing admin privileges for anyone else but themselves. Once a threat actor owns your entire network, there's not much you can do to stop them.

7 Asset Management

It's happened in many incident response engagements. The IR professional asks for an asset list to help determine the impact of the breach and gets a short answer from the organization's leadership: We don't have one. It's imperative for all organizations to have an asset list that includes physical assets such as devices and servers, and all data assets. During a data breach or data exfiltration investigation, knowing where your sensitive data is stored is critical to a timely investigation. It's hard to determine impact and report on progress to senior leadership if you don't know what data could have been compromised in the first place.

Proper asset management can help reduce your liability when it comes to notifying customers in the case of a breach

The more knowledge you have on the data you are storing, the easier it is to respond to a potential incident. Proper asset management can help reduce your liability when it comes to notifying customers in the case of a breach. For example, imagine a healthcare organization was breached and discovered it had many old patient records that were not needed but were still impacted. Even though those people are not current patients, the organization is still obligated to notify them of the breach. Good asset management can help streamline responsibilities and reduce the impact of a breach.

8

Segmentation and Architecture

Breaching an organization's cyber defenses is typically phase one of a threat actor's attack. In order to elevate their privileges and seek out the most valuable data, as well as deploy any ransomware, a threat actor must traverse the network. Having the proper segmentation and architecture is like placing hurdles in your network that the threat actor must jump over to succeed. Making the threat actor do more work and make more noise to compromise your systems should help you detect them sooner in the kill chain process.

Your system's architecture should be designed with the principles of confidentiality, integrity, availability, and resiliency in mind. Both system-to-system access and system-to-user access should be set up as a Zero-Trust model, where every transaction is authenticated with who and what the requester is and what permissions they have.

Controls That Ensure Rapid Response

Ensuring your security team can operate efficiently both before and after an attack will go a long way to reduce risk and improve performance when the pressure is on. These controls can help minimize the impact of a breach.

9

Extended Detection and Response

Extended detection and response (XDR) is a relatively new tool in cybersecurity that provides a full view of your attack surface and integrates it into one platform. XDR goes beyond endpoints to ingest and correlate network, cloud, identity and email sources and bring them all together into a single data lake for advanced detection, investigation and automated response. XDR consolidates multiple security controls into a unified platform that eliminates "swivel chair" scenarios where analysts must go between solutions to get all the necessary data for an investigation. A complete XDR solution will provide centralized prevention, detection, and incident response capabilities to address unknown, sophisticated threats and will boost operational efficiencies and analyst productivity. To do so, it should be extensible integrating with a variety of connectors and integration points. It will also include automated correlation and alert validation to reduce alert fatigue and allow security teams to place more focus on the threats that really matter.

A complete XDR solution will provide centralized prevention, detection, and incident response capabilities

Without XDR, analysts must take in alerts from all their disparate tools — antivirus, firewall, endpoint, network, cloud, identity management, etc. — and all of them must be treated as a true positive before being proven otherwise. Also, investigations take more time and detections are missed as there is no ability to correlate potential threat actor behavior across control points and escalate as a higher potential threat. On the response side, actions can be streamlined and automated to drive faster response. XDR brings all security controls into a single view and applies the analytics needed to driver greater accuracy and efficiency in detecting, investigating, and responding to threats.

10 Backup and Business Continuity

If an incident requires you to rebuild your systems, having a good business continuity plan with good backups will make a huge difference in returning your organization to normal. But what constitutes "good" backups? First, they need to be validated and tested so you can trust they have integrity and will restore what they are meant to restore. Many organizations have found out too late that their backups won't restore everything because of how they were set up, and now their plans to be up and running in a short amount of time have just been extended to weeks of inefficient and half-restored systems.

But what constitutes "good" backups? Many organizations have found out too late that their backups won't restore everything

In addition, backups need out-of-band authentication, which is a secondary verification method through a separate communication channel. Without this, a threat actor who gains control of your environment could wipe out your backups as part of their plans. If your backups are going to do you any good, they must be kept out of the hands of any threat actor.

From Holistic View to Holistic Approach

Implementing these security controls will no doubt raise the cybersecurity posture of your organization, but it's important to remember that the strongest cybersecurity comes from the right mix of people, processes and technology. Solutions and applications can only get you so far without a proper strategy in place, and a strategy needs people who can develop it, enact it, and adjust if needed in the heat of an incident. Your organization's cybersecurity risk will never be static, and reducing risk for the long term requires a comprehensive approach that understands that in cybersecurity, the whole is greater than the sum of its parts.

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of over 4,000 organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

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