Avast Business

White paper

Modernize your cybersecurity now: 10 reasons why and 10 ways how

16 September 2021

About the author

Rob Krug,
Senior Security Architect,
Avast Business

Rob has been in the network engineering and security space for over 30 years. His background includes extensive work with telecommunications, network design and management, and most importantly, network security. Specializing in security vulnerabilities, Rob has extensive experience in cryptography, ethical hacking, and reverse engineering of malware. Rob served in the U.S. Navy and also worked as a Data Security Analyst and Director of Engineering for multiple international service providers and vendors. Rob has designed, implemented, and maintained some of the most complex and secure networks imaginable.

Let's face it. Your organization is probably not doing all it could be to secure your users and IT resources. You know all about the high-profile hacks and exploited vulnerabilities, and you're of course concerned. But security is not the only thing consuming your organization's limited resources, and besides, you haven't been seriously breached. So far, anyway.

As other companies have learned the hard way, hope is a valuable human trait, but it's not a firm foundation for a security strategy. Fortunately, there are compelling reasons to focus on improving your enterprise's security and steps you can start taking today to do so significantly.

10 Reasons to Modernize Your Cybersecurity Now

1 Reduce risk

More effective, layered, and pervasive security will provide better protection for your users and IT resources. This reduces multiple risks, such as the risk of being breached or failing an audit.

2 Minimize IT and security costs

The 2015 Cost of Data Breach Study, conducted by Ponemon Institute and sponsored by IBM, surveyed more than 1,500 IT, compliance, and information security practitioners at 350 organizations in 11 countries. The study found that the average consolidated total cost of a data breach is $3.8 million, a 23 percent increase since 2013. Furthermore, the cost incurred for each lost or stolen record containing sensitive and confidential information increased six percent from a consolidated average of $145 to $154. Improved security also reduces the time and money required to remediate successfully exploited vulnerabilities, and enables better and more frequent cost-curbing automation.

3 Protect in silence

Modern, truly effective security is pervasive, ubiquitous, and invisible, with little to no impact on user productivity or business operations. The ability to improve security without disruption is essential to user satisfaction and the broad adoption of new features and tools.

4 See more, know more, and protect more

Maximum protection requires maximum visibility into and knowledge about your IT environment and its security posture. Only modern, integrated tools can provide this, empowering you to deliver the best possible security across your environment and organization.

5 Boost agility

Your organization must become and remain agile to survive and thrive competitively. Simply put, there is no agility without comprehensive, consistent security.

6 Increase enterprise resilience

A 2013 Ponemon Institute study sponsored by Emerson Network Power found that data center downtime costs approximately $7,900 every minute. A 2014 study conducted by Avaya found that each incident of downtime costs between $140,000 and $540,000, depending on the size and type of enterprise affected. And a 2015 survey by Kaspersky Lab and B2B International found that it can cost from $38,000 to $551,000 dollars to recover from a single cybersecurity breach. Statistics such as these build resilience - that is, your company's ability to minimize planned and unplanned downtime - an absolute necessity.

Emerson Network Power found that data center downtime costs approximately **$7,900 every minute.** A 2014 study conducted by Avaya found that each incident of **downtime costs between $140,000 and $540,000,** depending on the size and type of enterprise affected.

7 Develop trustworthiness

Edelman, the world's largest PR firm, surveyed some 33,000 people for its 2015 Trust Barometer. Some 63 percent of respondents said they simply will not do business with those they do not trust, while 80 percent said they only do business with trustworthy people and companies. And without modern, effective security, it is difficult or impossible to assure and demonstrate trustworthiness.

8 Enable user-centric security

Modern, user-centric IT focuses less on devices, files, and tools, and more on the user experience. To achieve user-centric IT, your company needs user-centric security—layered, integrated protection of all authorized users, resources, connections, and devices.

9 Operationalize security

Modern security management is less reactive and tactical, and more operationally focused and proactive. At larger organizations, operations personnel are increasingly performing security-related functions, enabling security specialists to focus more sharply on more complex and strategic issues. For small and mid-sized organizations, the trend is to move away from reactive "firefighting" and toward continuous delivery of new and improved security measures and more effective, proactive security operations (or "SecOps").

10 Prepare for the future

According to the Verizon 2015 Data Breach Investigations Report, some 70 percent of malware activity a decade ago was accounted for by only seven families or types of malware. By 2014, that 70 percent of malware activity was distributed across 20 different malware types. During this same period, malware evolved significantly, from email "worms" to "stealthy command-and-control botnet membership, credential theft, and some form of fraud." That same study estimates that five malware events take place every second of every day. Only modern, layered, user-centric security can provide the protection and adaptability your company needs today and will need tomorrow.

10 Ways to Modernize Your Cybersecurity Now

Implement consistently timely and comprehensive patching for all of your critical:

1 Operating systems

2 Third-party applications

-and-

3 Devices throughout your network, whether they're local, remote, or mobile

4 Establish non-intrusive, non-disruptive application whitelisting (and blacklisting, where needed)

If you do nothing more than the four steps above, you can make great strides toward improving security and protection at your organization.

According to the Australian Signals Directorate, **up to 85% of targeted attacks** can be prevented by whitelisting, patching operating systems and third-party applications, and restricting administrative privileges.

5 Automate as much of your proven patch and security management processes as possible

This will maximize the consistency of execution and scalability of those processes.

6 Integrate proactive patch management into and with all of your organization's other significant IT initiatives, especially those focused on IT Asset Management (ITAM), IT Operations Management (ITOM), or IT Service Management (ITSM)

Layered, effective, user-centric security is essential to the success of such efforts.

According to the U.S. National Vulnerability Database, **86% of reported vulnerabilities** come from third-party applications.

7 Engage, educate, and motivate users to understand the criticality of effective security

Your users are your first and last lines of defense. Comprehensive, effective, user-centric security seeks to protect them from being victims of malefactors and conduits of wrongdoing. It also encourages users (including customers) to report incidents and suspicious behaviors to IT support, security, or both, as soon as possible.

According to the Verizon 2015 Data Breach Investigations Report, **99.9% of the exploited vulnerabilities** in 2014 were compromised more than a year after the vulnerability was published.

8 Don't do it alone

Companies are increasingly deciding that the importance and rising demand for effective IT security is too much to be left in the hands of IT and security teams alone. Many are also separating security budgets and activities from mainstream IT, spreading those budgets, efforts, and awareness across the entire organization. Some well-known, highly respected companies are on record as "crowdsourcing" security information and intelligence. You can start by engaging colleagues in other departments within your own organization.

A Ponemon Institute/IBM survey of some 200 customers who have been breached found that only **45% of those breaches** were caused by malicious activities or software. The other **55% were caused by operational mistakes,** inadvertent errors by legitimate users, or problems with systems.

9 Use intelligence about your environment and tailored reports to identify and prioritize threats, to promote and encourage support of security initiatives, and to drive and support security-related decisions

Infrastructure intelligence and reports based on "real-life" data from your own environment can often be the most persuasive and effective communications tools with your colleagues within and beyond your IT and security teams.

10 Strive to make continuing education as an evolution of security at your company a priority for everyone

As Gartner analyst Lawrence Pingree told The New York Times in October 2015, "There are 600 million individual files known to be good, and a malware universe of about 400 million files. But there's also 100 million pieces of potentially unwanted adware, and 200 million software packages that just aren't known. It takes a lot of talent to figure out what's normal and what isn't."

You have no way of knowing if and when any of those 400 million known malware files may be targeted at your organization - if one of them hasn't been so already. And despite organizations spending some $30 billion annually on security tools, vulnerabilities and threats turn into actual breaches every day. By modernizing your IT security tools and processes, you and your team can materially improve security in ways that extend protections today and prepare effectively for the future, whatever it may hold.

Avast Business - All-in-one cybersecurity for the modern workplace

Avast Business offers multi-layered protection to safeguard your users and IT resources against the most sophisticated threats. Solutions include next-gen antivirus, automated patch testing, deployment, and management for Microsoft Windows systems and third-party applications, cloud backup, secure web gateways, zero trust network access, and more.

Our solutions are integrated in a single security platform. This enables rapid automation of both security and IT management policies, and delivers unequaled visibility across IT security and management activities.

Avast Business' security platform also delivers comprehensive, configurable reports and dashboard options. These help to sharpen risk and threat visibility, ease compliance with regulations and policies, and improve your overall security posture. For more information contact your Avast Business Account Manager or visit **www.avast.com/business**.