2023 GLOBAL CYBER CONFIDENCE INDEX

Cybersecurity Debt Drives Up Costs and Ransomware Risk

The research demonstrates the high cost of cybersecurity debt by showing how the cybersecurity debt associated with weak cyber hygiene practices is a leading cause of cyber incidents, including ransomware.

Cybersecurity debt refers to the unaddressed security vulnerabilities that pile up in organizations' IT environments. This debt accumulates from unpatched software, unmanaged devices, shadow IT, use of insecure network protocols, and more. Collectively, it adds up to all the access points attackers could exploit to compromise an organization, and it tends to undermine CISO confidence.

Cybersecurity debt often stems from weak cyber hygiene practices, but it also accrues over the course of normal business activity, as organizations adopt new technologies, enter into mergers and acquisitions, and onboard new employees, vendors and partners.

Many CISOs have long struggled to articulate the cost of cybersecurity debt to their organizations. Yet doing so is key to getting the funding required to pay down this debt, since it can expose organizations to significant risk.

To put the cost of cybersecurity debt into perspective and help security leaders make a compelling case for addressing it, ExtraHop partnered with Wakefield Research to survey 950 IT decision makers across the U.S., Europe and Asia-Pacific about the impact of cybersecurity debt on their organizations' security postures and their confidence in it.

Specifically, we asked IT decision makers about their organizations' use of certain network protocols (SMBv1, NTLM and LLMNR), about their practices for managing critical devices, and about the impact of these practices and protocols on their cybersecurity posture.

The research findings demonstrate a tight link between cybersecurity debt and heightened exposure to cybersecurity incidents, including ransomware. Our findings also help to show how weak cyber hygiene creates inefficiencies for security teams, and ultimately, leads to higher costs.

We know how difficult it is to address cybersecurity debt and improve cyber hygiene, and we understand the tradeoffs organizations are often forced to make between cybersecurity and business goals. This research will arm security leaders with the data they need to convince senior management of the value of paying down cybersecurity debt.

Number of ransomware incidents increased five fold from 2021 to 2022.

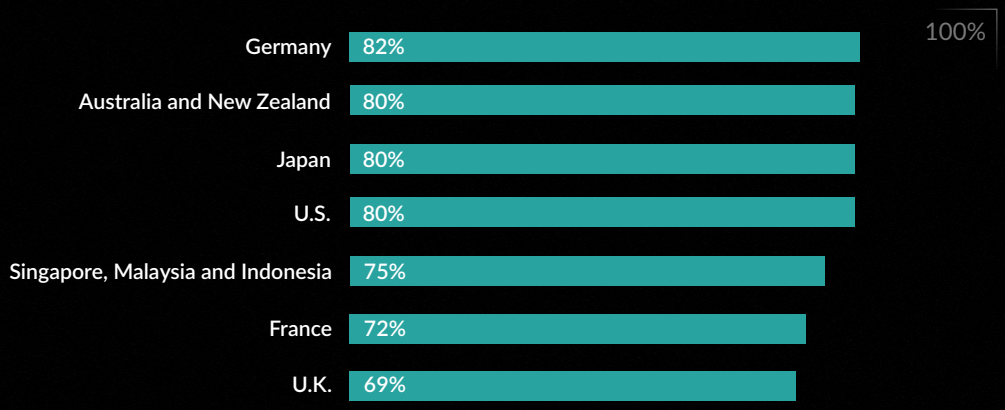
Data from our 2023 Global Cyber Confidence Index ties a direct link between cybersecurity debt and cybersecurity incidents, including ransomware.

More than three-fourths (77%) of IT decision makers say outdated cybersecurity practices have contributed to at least half the cybersecurity incidents their organizations have experienced. At the same time, the average number of ransomware incidents U.S. and European organizations[1] experienced in 2021 increased from an average of four attacks over five years to four attacks over the course of one year in 2022.

Despite government authorities like the FBI and CISA advising organizations against paying the ransom demand, data from the study shows an increase in the number of organizations paying the ransom, with 83% of respondents paying at least once.

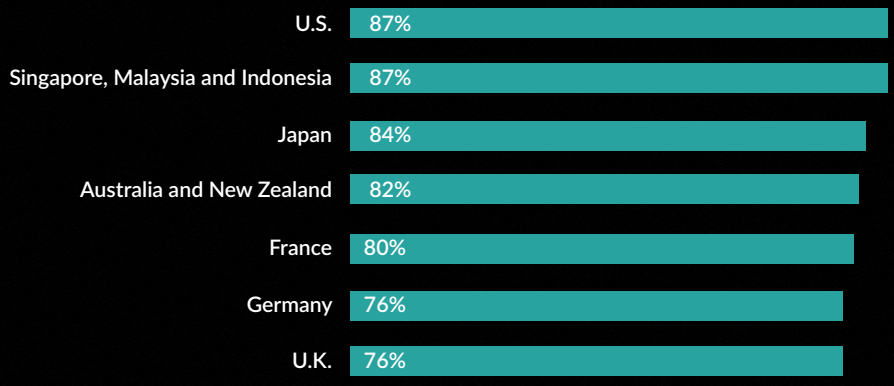
77%

of respondents say outdated cybersecurity practices have contributed to at least half their organization's cybersecurity incidents



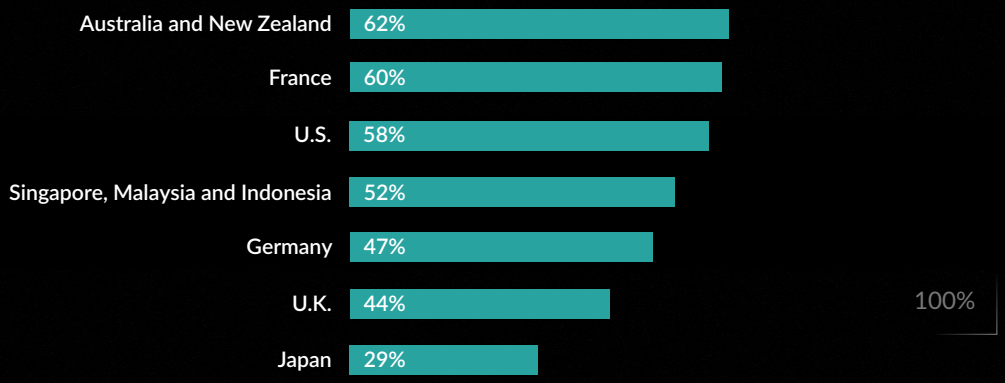
83%

of companies hit with ransomware paid the ransom demand at least once



52%

pay the ransom most or all of the time, up 12% from 2021



[1]The year-over-year comparisons shown throughout this report are representative of the U.S. and Europe only. The Asia-Pacific countries were surveyed only as part of the 2022 study, so no comparison data is available for them.

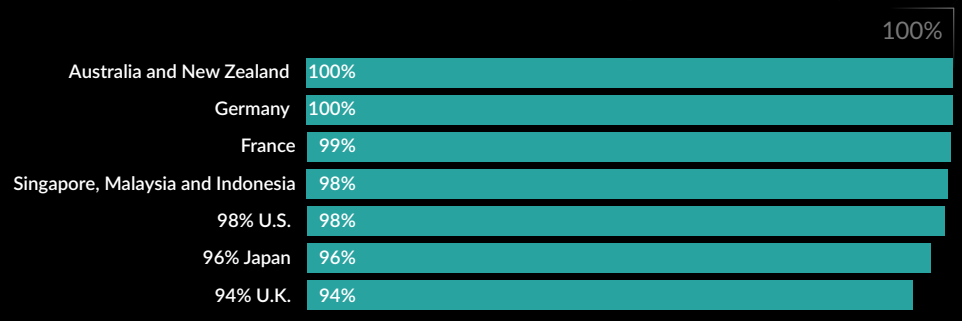
If an attacker can successfully access a server with SMBv1 enabled, they can quickly spread malware to other unpatched servers across a network.

Our study found significant gaps in organizations' basic security practices. For example, an overwhelming majority of respondents continue to run old, vulnerable network protocols like SMBv1, NTLM, and LLMNR. These protocols contain security vulnerabilities that are frequently exploited by threat actors, making them one of the weakest links in an enterprise.

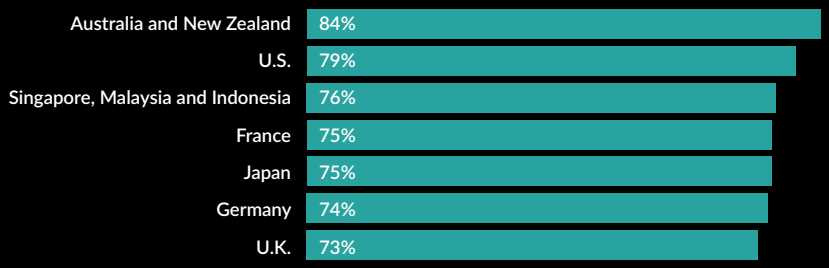
Vulnerabilities in SMBv1 were notoriously exploited in the WannaCry and NotPetya ransomware attacks. If an attacker can successfully access a server with SMBv1 enabled, they can quickly spread malware to other unpatched servers across a network.

Meanwhile, an attacker can use the LLMNR protocol to gain access to user credential hashes, which can then be cracked to reveal actual credentials. Attackers can also easily intercept NTLM hashes that are equivalent to passwords or crack NTLMv1 passwords offline.

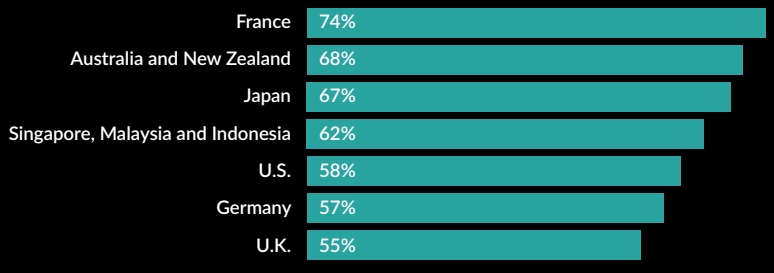
98%
say their organizations are running one or more insecure network protocols



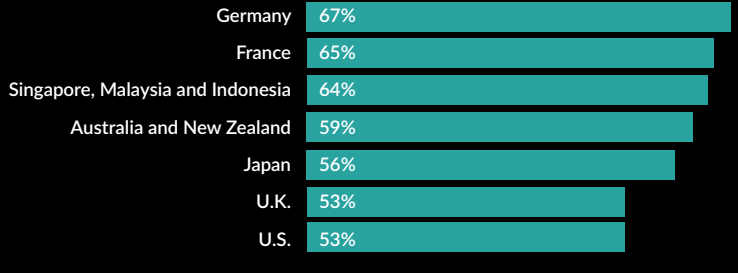
77%
run SMBv1, an increase of 8% over 2021



62%
run NTLM, an increase of 11% over 2021



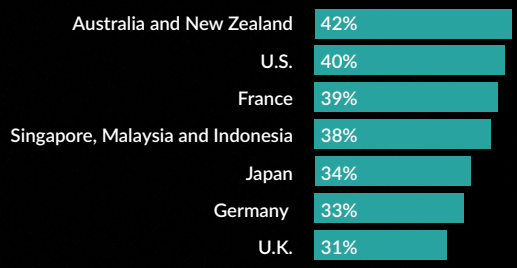
58%
run LLMNR, an increase of 10% over 2021



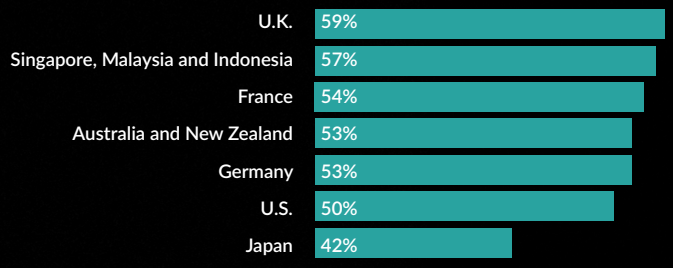
The other major cyber hygiene gap the study uncovered pertained to unmanaged devices. Respondents have a disconcerting number of unmanaged devices in their IT environments, including critical devices, such as database servers and domain controllers, that are either exposed to the public internet or capable of being remotely managed and controlled.

23%
of devices are unmanaged

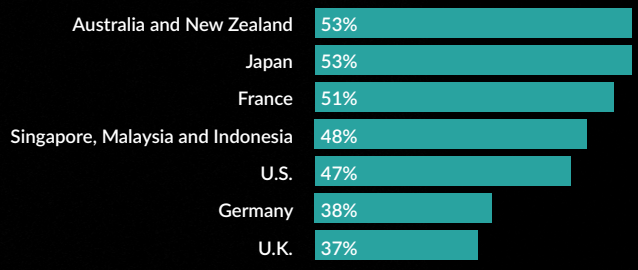
37%
say some of their organization's critical devices are unmanaged



53%
say some of their critical devices are capable of being remotely accessed and controlled



47%
say their critical devices are exposed to the public internet



Given that so many cybersecurity incidents stem from weak cyber hygiene practices and years of accumulated cybersecurity debt, it's not a stretch to put the cost of cybersecurity debt on par with the cost of a cyberattack.

$4.35M

Average cost of a data breach

Source: IBM Security, "Cost of a Data Breach Report 2022"

$4.54M

Average cost of a ransomware attack, excluding the ransom payment

Source: IBM Security, "Cost of a Data Breach Report 2022"

$925,000

Average ransom payment

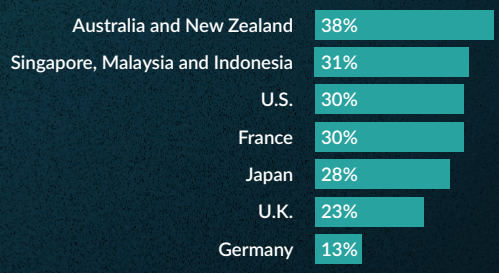
Source: Palo Alto Networks Unit42

Despite the direct link between costly cyber incidents like ransomware and poor cyber hygiene, fewer than one-third of the 77% of respondents who said half their cyber incidents stemmed from outdated security practices have immediate plans to address any of the practices that put their organizations at risk.

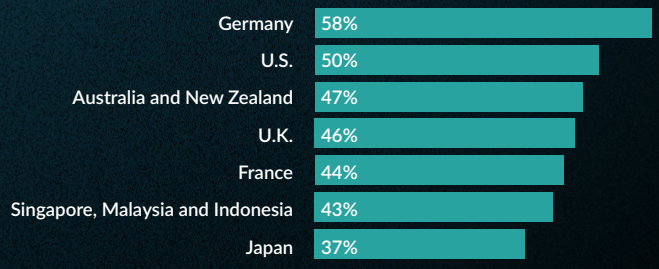
The one bright spot in the survey pertained to cloud workload security. More than half of respondents (52%) said they were mostly confident in the security of their organization's cloud workloads, with another 20% saying they were completely confident in them.

Of the 77% of respondents who said half their cyber incidents stemmed from outdated security practices:

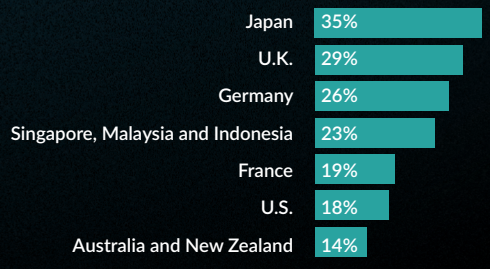
29%
plan to address those practices urgently



46%
say they'll update some of the outdated security practices as they get around to them



23%
say they'll likely only update a few of these practices as they become untenable risks



It's not a complete surprise that so few organizations have urgent plans to address outdated security practices. Afterall, many IT and security organizations are struggling with staffing and budget shortages. It's also notoriously difficult to transition from outdated network protocols, especially if large numbers of legacy systems rely on them to communicate. However, the risks and costs associated with running insecure protocols and other activities that compound cybersecurity debt may outweigh the effort required to update them.

Step 1: Perform Continuous Network Monitoring

Maintaining an inventory of software and hardware in your environment is a fundamental necessity for security hygiene, and is recommended in the first and second security controls in the CIS Top 20. Despite being a vital security practice, maintaining this inventory is a challenge for organizations that rely on manual, point-in-time audits to identify devices and protocols on their networks.

A better approach is to use a network monitoring tool that passively and continuously analyzes network traffic to pinpoint every device connecting to your network and each protocol in use at any given moment. The increase in both remote work and cloud environments has created more ways to introduce insecure protocols into organization's environments. These trends have made continuous monitoring of network traffic for device protocol identification essential.

Step 2: Update Configuration Templates and Settings

Devices and software that communicate across the network are configured with default settings that may go out of date over time. If a new device or solution is introduced into the environment and left to its default configuration, it may run protocols that are no longer considered secure.

Similarly, cloud systems and workloads use configuration templates to determine their protocol usage. Over time, as new protocols are developed and old versions deprecated, these configuration templates may go out of date and need to be updated. Any new workloads created with an older template may introduce insecure protocols into the environment. Because of the often short-lived and ephemeral nature of cloud workloads, it can be very challenging to catch these instances of insecure protocol usage and know how to get them out of your system. This is where a network monitoring solution can help.

Step 3: Disable Unused Ports

Other steps organizations can take to remediate network-related cybersecurity debt is to disable unused ports, as well as any unnecessary services, on internet connected networking devices, and of course, to develop and implement a roadmap for replacing legacy protocols.

The network delivers a powerful source of truth and transparency across all assets in an enterprise, from cloud to on-premises to endpoints. The network sees everything, shows everything, and leaves attackers with nowhere to hide.

Organizations can tap into the power of their network to reveal the "cyber truth" about threats and vulnerabilities in their environment using a network detection and response (NDR) solution. Through passive analysis of wire data, NDR platforms can reveal every user, application, asset, transaction, service and workload communicating with the network, including unmanaged devices, IoT devices, rogue instances, and shadow IT. NDR platforms can also show all the devices running outdated protocols, connected to the public internet, and capable of being remotely accessed and controlled.

By bringing all of these vulnerabilities to light, NDR plays an essential role in helping organizations improve cyber hygiene and confidence, and get on a path to paying down cybersecurity debt.

For more information, explore the role of NDR in your cybersecurity strategy.

The ExtraHop Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 950 IT decision-makers, director level and above, in the U.S., U.K., France, Germany, Australia/New Zealand, Japan, and Singapore, Malaysia and Indonesia between November 2 and November 13, 2022, using an email invitation and an online survey. Quotas were set for 200 respondents in the U.S., 50 respondents in Malaysia, and 100 respondents in each of the remaining markets.

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal the unknown and unmask the truth. The company's Reveal(x) 360 platform is the only network detection and response solution that delivers the 360-degree visibility needed to uncover the cyber truth. When organizations have full network transparency with ExtraHop, they see more, know more, and stop more cyberattacks. Learn more at www.extrahop.com.

ExtraHop

info@extrahop.com

www.extrahop.com