ExtraHop

CYBER CONFIDENCE INDEX 2022

Security Leaders are Confident, But Ransomware Attacks Tell a Different Story

An ExtraHop Survey of IT Decision Makers in the US, UK, France, and Germany

A recent survey of 500 security and IT decision makers in the US, UK, France, and Germany finds leaders highly confident about their organizations' IT security readiness, but admissions of lax security practices, combined with startling data about the frequency of ransomware attacks, indicate that the confidence may be misplaced. Those lax security practices include the continued use of decades-old networking protocols known to be used by ransomware. They also include high numbers of unmanaged devices, leaving critical data and IT resources exposed.

Survey highlights include:

- 77% of IT decision makers (ITDMs) are very or extremely confident in their company's ability to prevent or mitigate cybersecurity threats. And yet...
- 64% admit that half (or more) of their cybersecurity incidents are the result of their own outdated IT security postures.
- 85% reported having suffered at least one ransomware attack in the past five years, and 74% have experienced multiple attacks.
- 42% of companies that suffered a ransomware attack said they paid the ransom demanded most or all of the time.
- Why are these ransomware attacks succeeding? The survey revealed that organizations are still running old network protocols with little or no security controls. For example, 68% of ITDMs admit to running SMBv1, a file sharing protocol that Microsoft introduced in 1996. Worldwide, this protocol has led to over $1 billion in damages from cyberattacks.

The survey conducted by Wakefield Research—and sponsored by ExtraHop—explores how IT and security decision makers would assess their current security practices. It also delves into how frequently organizations are compromised by advanced threats like the new class of ransomware that has emerged over the last two years. Survey participants came from a wide range of industries, including financial services, healthcare, manufacturing, and retail, and worked at companies of varying sizes, including companies with annual revenue exceeding $50 million. About half the participants were in the US, with the rest hailing from the UK, France, and Germany.

Assessing Security Confidence and Practices in Today's IT World

The survey shows that however capable IT organizations have been in managing the dramatic transformations of the past couple of years, confidence still tends to outstrip actual security posture.

Responding to the pandemic, many organizations have switched to a work from home (WFH) model that allows employees to work remotely most or all of the time. This shift has also accelerated adoption of cloud services. Many organizations have used this occasion to modernize their IT infrastructures, finally decommissioning old on-premises applications, and replacing them with new SaaS applications or other solutions.

But they didn't modernize their protocol use: 69% are transmitting sensitive data over unencrypted HTTP connections instead of more secure HTTPS connections. Another 68% are still running SMBv1, the protocol that WannaCry and NotPetya ransomware variants use to infect corporate networks.

This data is supported by proprietary research from ExtraHop. In a June 2021 report, the company found that SMBv1 was in use in 67% of environments, consistent with the self-reported data from the survey. By contrast, ExtraHop's research found that 81% of organizations were running HTTP, suggesting that the continued use of this protocol may be underestimated by security and IT leaders.

Cyber criminals have been busy, too. While the first half of 2020 saw a huge spike in phishing attacks targeting remote employees, ransomware attackers didn't just advance their techniques for initial intrusion. In 2021, ransomware syndicates, including Darkside, REvil, and others, demonstrated advanced lateral techniques, including the golden ticket and living-off-the-land attacks. These tactics allow them to dwell in victim environments longer and inflict far more extensive damage, including exfiltrating data before encrypting it ("double extortion") and, in the case of Kaseya, also compromising victims' software in a supply chain attack that targeted thousands of customer environments.

Given the speed with which attack techniques have advanced, combined with increasingly remote workforces and an explosion of unmanaged IoT devices, we might expect to find ITDMs concerned about the state of their organization's security posture. We might also expect to see them embarking on modernization projects that include the abandoning of old network protocols known to be vulnerable. But our survey found the opposite: strong confidence in IT defenses, even while continuing to use decades-old protocols that security experts have been warning about for years. Let's look at these findings in detail.

Confident, but Compromised

Over three-quarters of ITDMs are completely confident (38%) or very confident (39%) in their company's ability to prevent and mitigate cybersecurity threats. Lack of confidence is rare: Only 4% are "only a little confident" and 1% are "not confident at all" in their company's cybersecurity abilities.

What's behind that confidence?

- 61% cited their company's commitment to best practices and secure processes
- 59% cited the security solutions they've adopted and implemented
- 55% cited the vigilance and ability of their IT team
- 35% said they'd faced major attacks before and patched their vulnerabilities
- 24% said they hadn't faced any "major" cyber attacks, so they weren't concerned

But some of this confidence seems misplaced. While respondents were overwhelmingly confident in their security posture, that confidence didn't translate when it came to ransomware attacks. The study revealed several important trends about ransomware, including the frequency of attacks, as well as how companies respond.

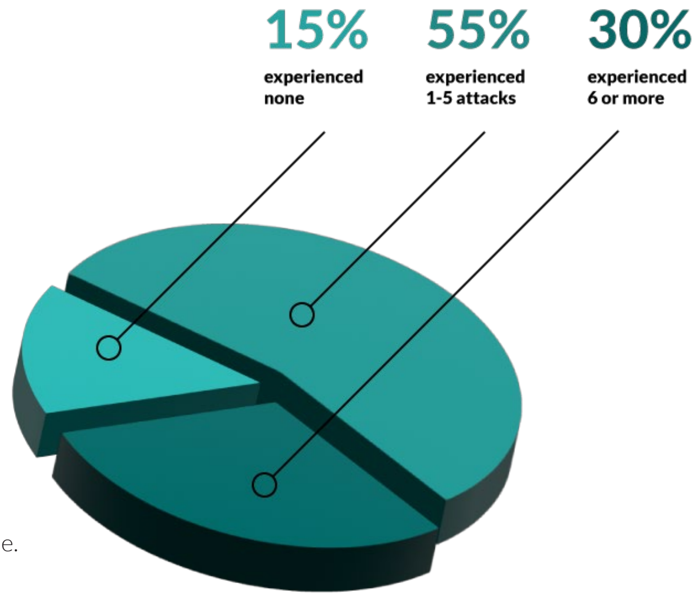
85% of companies are experiencing **at least one ransomware attack per year**

The Frequency of Ransomware Attacks

A small fraction—only 15%—of ITDMs reported never having experienced a ransomware attack in the past 5 years.

- 55% had experienced 1-5 attacks
- 30% had experienced 6 or more

This means that 85% of companies are, on average, experiencing at least one ransomware attack per year.



Unfortunately, Crime Pays

Not only are ransomware attacks prevalent, they're also overwhelmingly successful. When most companies experience ransomware incidents, they pay the ransom some or all of the time.

- 17% pay ransoms every time
- 25% pay most of the time
- 14% pay about half the time
- 28% never pay

The High Costs of Ransomware Attacks

The high costs of ransomware payments aren't the only damages that ransomware attacks impose. The survey asked the 85% of decision makers whose companies had experienced a ransomware attack in the past five years what kind of damage from ransomware they had experienced.

- 51% reported business downtime resulting from attacks on IT infrastructure
- 46% reported end user downtime resulting from attacks targeting users
- 45% reported IP loss, brand damage, fines, etc. resulting from data theft and leakage
- 44% reported business downtime resulting from attacks on OT infrastructure, such as medical devices, factory automation systems, etc.

Only 2% said they hadn't experienced any of these outcomes.

Ransomware: To Disclose or Not to Disclose

Companies were divided about 2 to 1 on whether it was "good to disclose when ransomware attacks happen to increase awareness and improve the ability to respond to future attacks."

- 66% agreed that it was good to disclose attacks
- 34% disagreed, preferring privacy

But when it came to actual disclosures, the numbers told a very different story. While two-thirds of respondents believed transparency around ransomware attacks was important, less than 40% said their organizations were fully forthcoming when the attacks took place.

- 39% said they were willing to make information available for public knowledge
- 34% let some people know, but didn't make information available to the public
- 27% limited the news as much as possible

The Sources of Risk

As the statistics shared here show, while security leaders and ITDMs are confident in their security posture, that confidence hasn't stopped ransomware attackers from gaining a foothold. The survey revealed key areas of weakness common across respondents.

Risk #1: Continued Use of Insecure Network Protocols

Decades ago, even technology leaders like Microsoft designed networking protocols and other technologies with little thought to IT security. Corporate environments were trusted environments. Software wasn't designed to withstand attacks from malicious users, let alone those with the resources of nation-states and military intelligence units––and, increasingly, resources that include a vault full of illicit cryptocurrency.

Today everyone knows that enterprise IT is under constant attack, and that cybercriminals will take advantage of any vulnerability in older technologies, like the Apache log4j logging utility. Plenty of other older technologies pose threats, too, including:

- SMBv1 (also known as CIFS), a Microsoft file-sharing protocol from the early days of the internet. Unfortunately, SMBv1 is still used in most SMBs and large enterprises. That's a problem, because some of the most damaging strains of malware like WannaCry and NotPetya use this insecure protocol to move laterally across networks.
- NT LAN Manager (NTLM) protocol, a challenge-response protocol used by servers to authenticate clients using password hashes. Unfortunately, NTLM doesn't support modern cryptographic methods such as AES or SHA-256, and it's vulnerable to brute force attacks.
- Link-Local Multicast Name Resolution (LLMNR) protocol, a DNS-free mechanism for host-name resolution within a local environment. Attackers can use LLMNR to trick a victim into revealing user credentials.
- HTTP, the original transport protocol for HTML traffic, which transmitted content without encryption. A best practice is to replace HTTP with HTTPS, a new protocol that does apply encryption. Unfortunately, HTTP is still widely used, as this survey found.

This survey asked ITDMs how many of these protocols they were still using, despite their confidence in their company's security practices. Surprisingly, the protocols are still widely used:

- 92% admitted running SMBv1, NTLM, or LLMNR in their environments
- 88% admitted still running HTTP, and 62% admitted running it often or sometimes
- 68% admitted running SMBv1
- 49% are running NTLM
- 48% are running LLMNR

Use of these protocols is inversely correlated with ITDMs' confidence. For example, ITDMs who are very or completely confident in their cybersecurity stance are much more likely (74%) to be running SMBv1 than their less confident peers (45%). A further irony about this confidence: Nearly 2 in 3 ITDMs (64%) admit about half or more of their cybersecurity incidents are a result of their own outdated security postures.

Budget isn't necessarily the issue here: 79% of companies with revenues of $50 million or more are still running SMBv1, while 60% of smaller companies are. Both numbers are dismaying, but the fact that larger companies tend to have greater instances of these protocols underscores how difficult it is to update entrenched and widely-used legacy systems.

Risk #2: Unmanaged Devices

Another area of concern is the number of devices, including employee laptops and desktops, as well as IoT devices, that are unmanaged by the IT organization. Unmanaged devices may be missing key security defenses such as AV or EDR software, and they're likely to be behind on their patches, making them susceptible to a broad range of attacks. On average, companies report that 29% of their devices are unmanaged.

- 27% report that 26-50% of their devices are unmanaged
- 11% report that 51-75% of their devices are unmanaged
- 5% report that (an astounding) 76-100% of their devices are unmanaged

> Taking weeks or longer to patch vulnerabilities
> **is highly risky behavior.**

Risk #3: Slow Response Times to Critical Vulnerabilities

When it comes to responding to critical vulnerabilities by installing patches or shutting down a vulnerable solution, response times vary:

- 26% respond in less than a day—probably fast enough to prevent most attacks
- 39% take one to three days
- 24% take up to a week
- 8% take up to a month
- 3% take longer than a month

For high-profile organizations already being targeted by attackers, taking weeks or longer to patch vulnerabilities is highly risky behavior.

IT Security Wish List:

Better Insights, the Right Data (But Not Too Much), and Improved Cooperation Among IT Departments

Nearly all security teams (94%) are facing challenges as they work to defend against ransomware and other forms of cyberattacks. When asked to identify their top challenges:

- 43% cited the lack of cooperation between their network, security, and cloud operations teams
- 40% cited a lack of investment
- 39% cited the long time required to train new hires
- 35% cited inadequate or overlapping tooling
- 29% cited low morale among team members

Some conclusions from this part of the survey: IT organizations need better tooling that will support improved collaboration among network, security, and cloud operations personnel.

What factors are hindering incident response efforts specifically? The most disruptive factors are:

- Too much data to find real insights
- Encryption obscuring valuable data points in network
- Lack of network and/or application visibility

IT organizations need more visibility, including access to data obscured by encryption. But they need that data delivered in a useful way so it doesn't add to the barrage of data, making it difficult to find insights.

Conclusion: Companies Are Caught Between Past and Future

This survey shows that even as companies continue to innovate with cloud technologies and remote workforces, their IT infrastructures remain mired in the past, with obsolete protocols providing ongoing opportunities for attackers to infiltrate networks and unleash ransomware attacks.

The obstacles to fixing these problems involve culture as much as they do budgets. IT organizations are looking for ways of working more quickly and collaboratively, bringing network teams, cloud teams, and security teams together to work effectively on threat reduction.

> They're missing the critical insights they need to identify vulnerabilities and **stop ransomware attacks from becoming an annual event.**

The obstacles also involve data. IT organizations are overwhelmed with data, yet they're missing the critical insights they need to identify vulnerabilities and stop ransomware attacks from becoming an annual event. Despite these challenges, the survey finds that most ITDMs are confident or highly confident about their company's security postures.

We hope that with the use of the right IT security solutions and practices—including the disabling of vulnerable protocols and more effective data-sharing among IT teams—security postures will improve. Then ransomware attacks will become less damaging and less frequent, and that bold confidence, so striking in the survey results, will come to be well-earned, not misplaced.

Findings by Region

While for the most part, the trends are consistent across the countries surveyed, we did note some key differences by region.

CISOS in the United States are the most confident in their ability to prevent and mitigate threats. 82% of US respondents are either completely or very confident.

- CISOs in the United States have also experienced more ransomware incidents. They report an average of 4.91 incidents in the past five years, and more than half of respondents from the US have paid ransom some or most of the time.
- But CISOs from the US are more likely to acknowledge the need for modernization, with 44% of US respondents admitting that more than half of all incidents are related to outdated security postures.

French CISOs report taking longer to respond to critical vulnerabilities, with 45% of respondents reporting response times of a week or more.

- France is also most likely to acknowledge staffing challenges, with 49% of respondents citing training and 46% of respondents citing talent availability as a top challenge.
- French CISOS are also the most likely to admit to having challenges in general, with 99% of respondents citing at least one.

UK CISOs are also more confident in their modern approach. 70% of respondents report that outdated security postures are related to half or fewer of all incidents.

- They back up their confidence by being the least likely to report unmanaged devices or use of insecure protocols—but usage of both is still high—with 89% of UK respondents using at least one insecure protocol.
- The UK reported experiencing fewer ransomware incidents on average, at 3.51 incidents in the past five years.

German CISOs are the least confident in their ability to prevent and mitigate threats.

- They're also the least likely to pay ransom—only 8% of German respondents admit to paying every time.
- But they aren't always open about breaches, with 69% of respondents admitting to not being fully open about disclosing attacks.

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

ExtraHop

info@extrahop.com
www.extrahop.com

© 2022 ExtraHop Networks, Inc. All rights reserved. ExtraHop is a registered trademark of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners.