ActualTech MEDIA

Hewlett Packard Enterprise

Cybersecurity Remains Mission Critical

Ed Tittel

CONTENTS

IN THIS PAPER

Organizations of all sizes struggle to stay ahead of a never-ending and always-increasing collection of security threats and vulnerabilities. Because they're cash- and resource-constrained, this hits small to midsize organizations particularly hard, and can even pose existential threats. Thus, such businesses need expert info, insight, and assistance to make sure they get cybersecurity right.

Highlights include:

- Explanation of common business circumstances that make cybersecurity challenging
- A quick review of five common security threats: phishing, malware, ransomware, date breaches, and compromised passwords
- Three good remedies to improve security posture by building cybersecurity expertise, improving user security awareness, and creating and enforcing security policy

The wild and digital world can be scary and challenging, especially for small to midsize businesses. As technologies become increasingly distributed and interconnected, the cyberthreat landscape continues to evolve and gain complexity and danger. Today's threats and vulnerabilities require business operators to take a highly systematic and strategic approach to security. That means they must identify and prioritize protection and defense of their most valued assets. These include their customers, their data, and their sources of revenue, as well as the IT infrastructure and systems that need dedicated, capable cyber defenses.

Security Is Key to Business Success

Given an ever-expanding threat landscape, security has become even more crucial to the effective operation for all business, including even the smallest of operations. Owing to the complex and ever-evolving nature of today's cyberattacks, small to midsize operations must understand what to do and what to watch out for. They must also understand how much proper protection costs, and the kinds of risks that must be prioritized and safeguarded against.

According to Forrester's State of Security Operations 2021, key business challenges include the following across all businesses:

- Security Operations teams struggle to address high alert volumes: less than half of decision makers say their organizations can address most or all the security alerts they receive daily. Teams struggle to triage and investigate threats quickly. Because of alert volume, teams must often ignore low-priority threats that still leave organizations vulnerable to risk so they can concentrate on urgent, high-priority matters.
- Nearly half of firms report difficulties hiring and retaining qualified security staff. Because so much threat detection, investigation, and response occur manually, security teams face high rates of analyst burnout. Teams are starting to automate workflows to alleviate this crunch. Smaller businesses generally face larger challenges finding good people, because bigger businesses can offer better packages (pay, benefits, and so forth).
- Almost 75% of decision makers have started Security Operation Center (SOC) automation—with full automation as a long-term goal. As of April 2021, 70% of organizations surveyed have started down this path. Also, 44% of that survey population expect increased automation in the coming year or two. Those who've adopted automation report more effective and cohesive SOC teams that face a lower likelihood of technical gotchas, including poor visibility into security issues and answers and lack of tool integration.

In general, smaller businesses feel the constraints and impacts related to security matters more keenly than larger ones. Indeed, the smallest of businesses (those with nine employees or fewer) very likely have neither a dedicated security resource, nor much in-house expertise when it comes to dealing with ongoing security issues and concerns. That makes access to security insight, resources, and services something of a must-have to such operations.

> **Given an ever-expanding threat landscape, security has become even more crucial to the effective operation for all business, including even the smallest of operations.**

Leading Security Threats

Security Magazine reports the five top cybersecurity threats in 2021 as the following (see **Figure 1**):

Phishing: an attack method that presents users with safe-seeming email or social media items that trick them into downloading harmful content. Phishing can look legitimate, and uses apparently safe links, attachments, names, and logos to persuade readers to click embedded links or download files or attachments. Spear phishing targets people who work in specific departments such as Finance, AP/AR, or Purchasing where theft might be possible. Whale phishing targets high-visibility targets (typically C-Level executives whose names and identities are public and known). Smishing uses SMS messages to

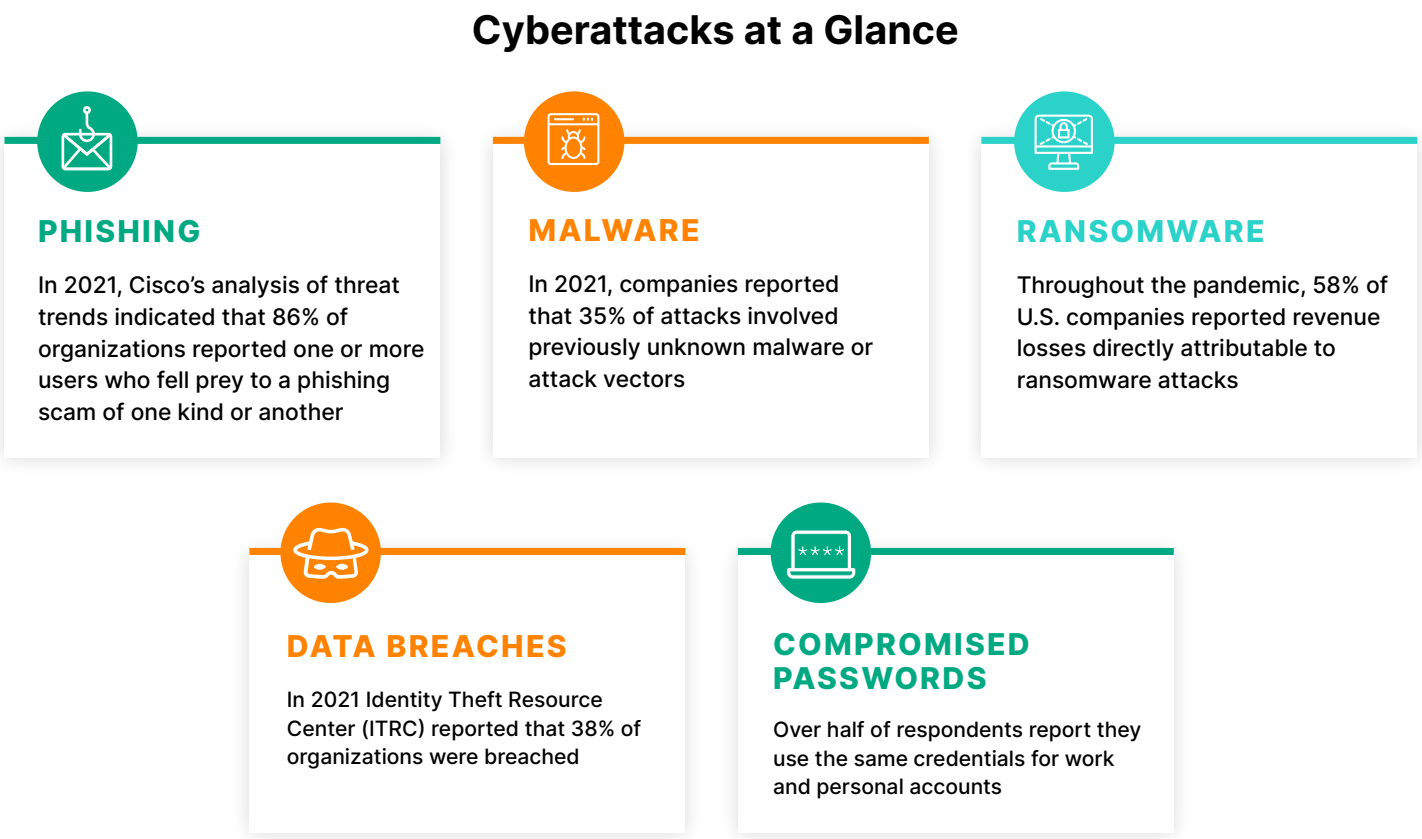

Figure 1: Security Magazine's top 5 cybersecurity threats in 2021

persuade readers to click malicious links. In 2021, Cisco's analysis of threat trends indicated that 86% of organizations reported one or more users who fell prey to a phishing scam of one kind or another.

Malware: Aka malicious software such as worms, viruses, Trojans, ransomware, adware, and so on, that attack devices to slow them down or stop them from working. Some malware also targets specific kinds of information that it seeks to exfiltrate to a malicious third party, such as accounts and passwords, credit card information, financial accounts, and more. Malware finds its way onto PCs via clicking a malicious link, downloading malicious files or software, clicking pop-up advertising, or opening unsolicited (and unexpected) email attachments. Once it's running on a targeted PC, malware can ransack systems and steal information. In 2021, companies reported that 35% of attacks involved previously unknown malware or attack vectors. That percentage is almost certain to grow as most of the workforce goes remote.

Ransomware: One of the most insidious and visible forms of malware, ransomware encrypts all files on systems it infects. It requires users to pay an often-hefty ransom for a decryption key so they can get their files back. Because not all decryption efforts succeed, the FBI recommends against paying such ransoms, though high-visibility companies like Colonial Pipeline ($3 million of which $2.3 million was later recovered) and a major insurer ($40 million) have found themselves forced to pay to regain access to systems and data. Throughout the pandemic, 58% of U.S. companies reported revenue losses directly attributable to ransomware attacks.

Data breaches: Unwanted and unauthorized disclosure of data, often customer account details and information (such as credit card numbers, SSNs, names and addresses, contact info, and so on), can occur when cyberattacks succeed, and hackers gain access to company systems and data. Breaches can occur through hacks into company networks or point-of-sale systems. A Q2 2021 analysis

from the Identity Theft Resource Center (ITRC) reported that 38% of organizations were breached. If a data breach occurs, businesses must respond immediately to contain its effects and resolve related issues. Failure to act can damage reputations and lead to fines into the millions of dollars.

Compromised passwords: Usually harvested when a user logs into a fake (but real-looking) website, user accounts and information can be accessed when such credentials become known.

In fact, there's a thriving trade in such information, because many users ignore security advice and use the same credentials on multiple (or all) of their online accounts. Over half of respondents report they use the same credentials for work and personal accounts. Companies must therefore teach workers how to create (and preserve) account and password security.

> **Two advantages of working with an outside company are that they can provide 24/7 monitoring for attacks that can occur anytime, and outside companies can bring in experts who always stay up-to-date on the ever-evolving threat landscape.**

Security Magazine also recommends three general approaches to handling such threats, all of which are eminently sensible and achievable:

Build cybersecurity expertise, internally and externally. For small to midsize operations, working with a freelancer or hiring an outside organization—like HPE and its partners—is a good option. Two advantages of working with an outside company are that they can provide 24/7 monitoring for attacks that can occur anytime, and outside companies can bring in experts who always stay up-to-date on the ever-evolving threat landscape.

Educate your team. Make sure everyone knows what's what and is on the same page. This includes raising general employee security awareness, and training those with security responsibility to work with service providers to recognize and react to threats quickly and directly. HPE and its partners can provide security awareness training and regularly assess employee security awareness with ready access to refresher and specific remedial training as needed. They can also work with designated members of your staff to handle alerts and fend off potential or actual attacks.

HPE has teamed up with global cybersecurity training champion SANS (an old acronym for System Administration, Audit, Networking and Security, and the name of a leading training provider for three decades) to offer outstanding security awareness training for employees. When used as part of new-hire onboarding, with regular, periodic refresher classes, security awareness helps organizations avoid all kinds of potential security trouble. For more details see HPE/SANS Security Awareness Training.

Create a cybersecurity policy. The basics of a workable security policy should include guidelines on protecting devices, multi-factor authentication, and data protection. This should be a living, constantly updated document that reflects the current state of threats and attacks. Here, again, HPE and its partners can help your organization adopt and maintain such a policy, and make sure it's properly enforced to deliver the protection and peace of mind your organization needs.

> **Educate your team. Make sure everyone knows what's what and is on the same page.**

Special Challenges for Smaller Businesses

Because they are often cash- and resource-constrained, smaller businesses are particularly subject to security issues and problems. Low staffing levels in general often mean that IT expertise is itself scarce, so that security expertise may either be entirely missing or seriously overstretched. Alas, this too often means that smaller businesses—particularly those with 100 or fewer employees—will be stuck in reactive mode, mostly unable to anticipate and head off security trouble before it becomes dangerous or poses risks to revenues or outright business viability.

> **Because they are often cash- and resource-constrained, smaller businesses are particularly subject to security issues and problems.**

In particular, small and midsize businesses may find themselves saddled with unwanted and unexpected Issues that can present when slow response time to threats or vulnerabilities hamper or restrict their productivity and profitability. When you stop to consider that IBM disclosed the average cost of a data breach in 2021 was a whopping $4.24 million, that could be more cost than many small to midsize businesses could survive intact.

> **Factoring in the added complications of remote work, and ever more distributed modes of operation and interaction, organizations need the kind of security help, insight, and assistance that HPE and its partners bring to the table.**

That's why small to midsize businesses should turn to HPE and its partner network to obtain security solutions and expertise. HPE is committed to helping such operations implement affordable and workable security so their businesses can survive—and even thrive—in today's rough-and-tumble digital world. Factoring in the added complications of remote work, and ever more distributed modes of operation and interaction, organizations need the kind of security help, insight, and assistance that HPE and its partners bring to the table.

LEARN MORE

Visit the HPE small and midsize business IT solutions center for more information about easy-to-own, ready-to-use and well-supported business technology solutions that turn servers, storage, software, networking, cloud, and security capabilities into a turnkey experience. HPE and its partners are ready to provide security information, insight, and assistance as needed.