KEYPOINT INTELLIGENCE

SERVICE AREA:

Business Development Strategies

ANALYSIS

THE CONVERGENCE OF SECURITY AND PRIVACY

WHY PSPS NEED TO PAY ATTENTION

FEBRUARY 2021

contents

Document

Figures

Introduction

The introduction and mass adoption of the internet ranks among the most disruptive events in human history. It has enabled businesses of all shapes and sizes to promote and sell their offerings, and it has also made a never-ending pool of knowledge accessible to anyone who knows where to look. As with so many other major transformations, however, there is a dark side to all this information. No sooner did the internet start to store valuable knowledge than criminals set out to steal it. Some techniques, like phishing, simply evolved from print to digital. Other types of attacks, however, were new and designed specifically with the digital landscape in mind. As more people started to use the internet, the rate of cybercrime continued to increase.

Of course, all of this was happening before the COVID-19 pandemic abruptly forced the majority of global businesses into online-based workflows. The global health crisis was the equivalent of a feeding frenzy for cybercriminals. Organizations with incredible amounts of personal and confidential data—many with no real experience/education on online infrastructures—were suddenly forced to depend on the internet for their daily businesses. This dependence actually extended beyond the internet, also encompassing remote-based, decentralized organizational structures and workflows.

The effects that COVID-19 had on cybercrime were grim but expected. In April 2020, the FBI reported that cybercrime was already up by 300%, with some experts believing the actual figure to be much higher than that.[1] The reality is that many organizations did not consider themselves targets of cybercrime, falsely believing that only financial institutions and government bodies needed to be concerned. As a result, many print service providers (PSPs) fail to understand that they are prime targets for cybercrime and cyberattacks.

As we continue through 2021, now is the time for action. PSPs that have not at least started to develop comprehensive cybersecurity strategies must do so before it is too late. According to a report from IBM[2], the average cost of a cyberattack in 2020 was nearly $4 million.

Why Cybersecurity Should Matter to PSPs

Many PSPs do not consider themselves at risk for advanced and dedicated cybercrime. The logic is that most printing companies simply do not have what cybercriminals are after (i.e., personal and confidential data that can yield a huge cashflow). This logic is flawed for a number of reasons. For starters, every company has employees—and their data can

[1] https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic
[2] https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

and is often targeted by cybercriminals. In addition, while print companies and PSPs do not have the data that a bank might, they frequently work with banks and other financial institutions. Digital security should be seen like a chain: If there is a weak link anywhere, the entire chain can break. Cybercriminals don't need to get directly into a financial institution's network if they can go in through another avenue, perhaps by stealing a PSP's network access and pretending to be the print partner.

Because they have access to incredibly powerful organizations, printing companies are prime targets for cybercrime whether they realize it or not. Printing companies can and should be viewed as onramps to a highway of personal and confidential data.

Understanding the Internet of (Potential) Threats

Today, more and more devices are becoming "smart." There are smart watches, smart televisions, smartphones, smart thermostats, smart refrigerators, and even smart irons… just to name a few. While artificial intelligence (AI) is fast becoming one of the most overused buzzwords around, intelligence in this case does not imply the presence of a brain. It is simply shorthand for online enabled. Every smart device can connect to the internet in some way, meaning they are all potential network access points. This bears repeating—all smart devices are potential network access points.

If you think of a network as a house, then each access point is a door. Many people think of their computer as the only network access point, but that simply isn't true anymore. Based on the list above, most of today's houses have lots of doors. In addition, there's another popular device that was network connected long before the term "smart" really caught on—the printer.

Companies such as HP have been sounding a warning bell for years that network-connected printers should not be overlooked when considering issues of cybersecurity.[3] As recently as August 2020, ethical hackers (people who seek exploits just to point out to businesses that said exploits exist) breached thousands of printers just to show that they could.[4] This "attack" was a very light distributed denial of service (DDoS). They essentially just sent each device a page or two of print. A true malicious attack would bombard the printers for hours or even days, grinding business to a halt while also causing lost productivity and potential printer hardware damage.

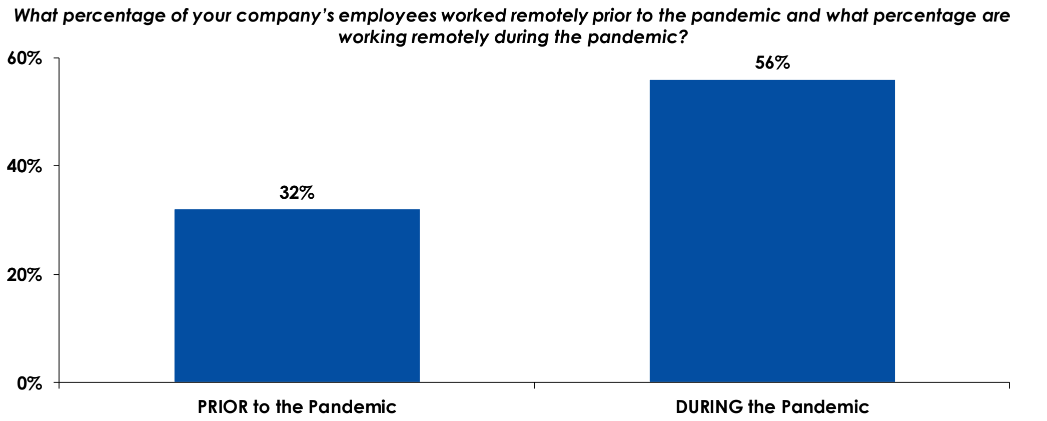
A strong cybersecurity presence involves understanding which devices must be protected, and that includes everything in the internet of things (IoT). Going forward, print companies should view IoT as not just things, but potential threats.

[3] https://www8.hp.com/us/en/security/cyber-security-center.html
[4] https://cybernews.com/security/we-hacked-28000-unsecured-printers-to-raise-awareness-of-printer-security-issues/

Challenges in a Decentralized Business World

As is the case with many other industries, COVID-19 has accelerated the pace of change in regard to business workflow. In particular, the pandemic took decades of academic discussions on the idea of remote work and transformed it into reality essentially overnight. Businesses that had spent years wondering if they could go remote suddenly had no choice. Data that Keypoint Intelligence gathered during a recent survey of small and medium-sized businesses (SMBs) uncovered a sizeable increase in remote work during the pandemic.

Figure 1: Remote Workflow Statistics



N = 350 Total SMB Respondents
Source: *Small/Medium-Sized Business (SMB) Print Buyer Survey;* Keypoint Intelligence 2020

While it is too early to say exactly how many workers will remain remote once the pandemic has subsided, Keypoint Intelligence believes that the number of post-COVID remote workers will be significantly higher than pre-2020 levels. If this proves to be the case, a greater strain will be placed on networks. While many companies are turning to cloud-based service providers for remote workflow, still others are forging ahead with their own solutions. The more work processes that go online, the greater the impact a cybercriminal can have on a business.

There's another danger as well—having remote-based employees means having less control over registered company devices. For instance, workers may use personal laptops, PCs, tablets, or smartphones to handle work-related tasks. Once these devices have gained access to the network, they themselves become new doors that can bypass security programs and get into confidential areas. If a remote employee is using his or her smartphone for business tasks without alerting anyone in the company, business security could be at risk if that device is lost. It is for this reason that many businesses have begun to rethink bring-your-own-device (BYOD) policies. In many cases, the security risks can outweigh the possible productivity gains.

If PSPs wish to transition to more remote-based workflows and decentralize their businesses, they must prepare for added cybersecurity risks and take the appropriate precautions. One commonly used cybersecurity method is the principle of least privilege. This IT strategy fundamentally builds a restricted network, one where any employee can access but few can see everything. Employees are instead only given permission to view relevant files and folders on the network. That way, if one employee is compromised, most of the network remains secure.

Education is a Great Precaution!

Many companies are concerned about the cost of effective, cutting-edge cybersecurity initiatives. It is no secret that COVID-19 hit the print industry hard, and many businesses have needed to make tough choices about their investments. While economic recovery will likely occur later in 2021, PSPs should not wait to invest in stronger cybersecurity practices. The good news is that one of the most effective ways to combat cybercrime is also among the least expensive.

According to data compiled by cybersecurity education firm Cybint Solutions, roughly 95% of all cybersecurity breaches are due to human error.[5] Cybercriminals cast wide nets—they aren't seeking to fool everyone, just the least informed. As such, cyberattacks rarely occur due to failures in the IT department or with IT staff. Instead, an unrelated employee may be lured in by a simple phishing scam.

Phishing is a cyberattack wherein the criminal sends an e-mail or text posing as someone else in the company (usually someone in a position of power). These communications often appear urgent, and they may state that information is vital to prevent disaster. There might be an element of threat involved too (e.g., "do this or you're fired!"). Phishing can be very intimidating to someone untrained, and this is by design. The last thing the criminal wants is for the would-be victim to think rationally. They want to provoke an emotional response, trigger an immediate action, and reap the benefits. Phishing is an incredibly common form of cyberattack. Spear phishing is an increasingly popular variant wherein the criminal goes the extra mile to make the message sound more targeted—and thus more believable. Cyber research firm Proofpoint found that 88% of organizations worldwide experienced spear phishing in 2019 alone.[6]

Luckily, there are usually way to tell if a message is fraudulent, and education can be your greatest protection against cybercrime. Teach your employees to look for the following:

[5] https://www.cybintsolutions.com/cyber-security-facts-stats/
[6] https://www.proofpoint.com/sites/default/files/gtd-pfpt-uk-tr-state-of-the-phish-2020-a4_final.pdf

- **Spelling mistakes**: Phishing e-mails rarely have the professionalism of genuine work e-mails. Furthermore, many are sent unedited, so multiple spelling or grammar errors may be present.

- **Wrong Web/Return Address**: Almost every business has an official web domain through which to handle e-mails. Because cybercriminals will lack access to this domain, their return address will commonly be suspect even if they claim to be from a particular company.

- **Unprofessional content**: Executives can save a lot of potential time and energy by setting clear rules that certain things should never be disclosed via e-mail. This way, if a cybercriminal requests sensitive information, such as a password or other network data, the employee will know enough not to divulge this information.

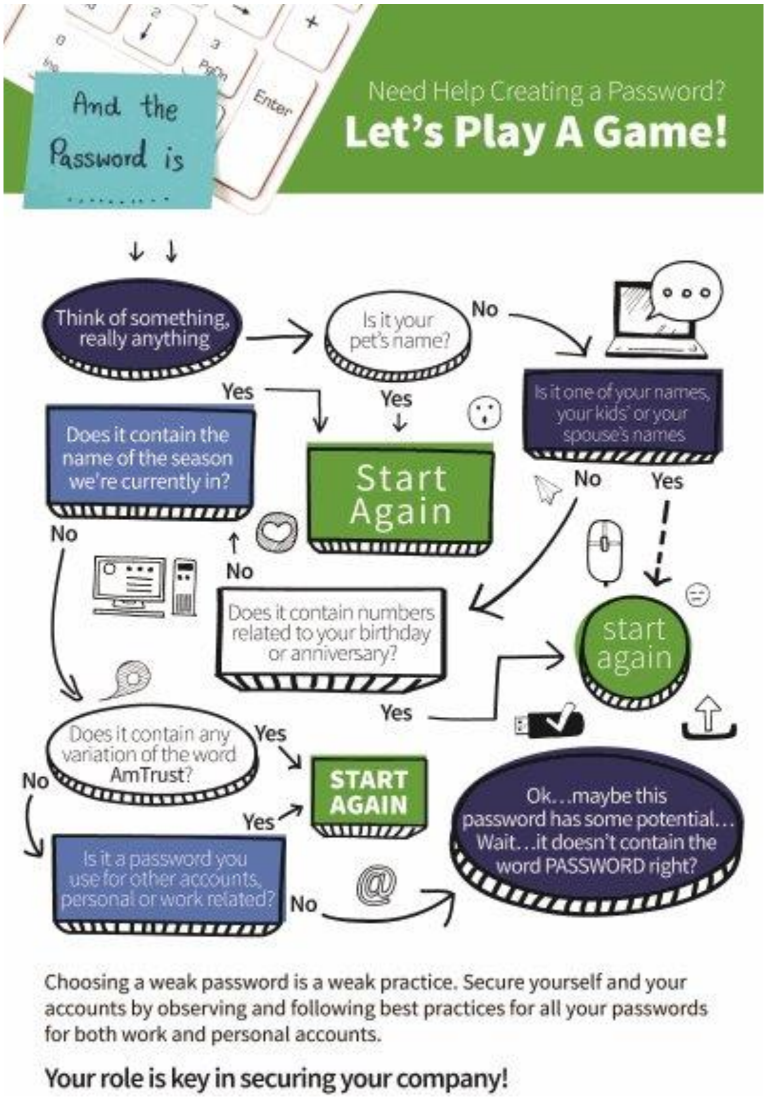
- **Urgency and links**: As noted earlier, phishing e-mails frequently demand immediate action. Many phishing e-mails will also contain links to malware. A good rule of thumb is to teach employees to forward suspect e-mails to an IT professional before taking any action or clicking any links.

Teaching employees about cyberattacks like phishing and training them to be register any hardware with network access will go a long way to cut down on the risks of a cyberattack.

There is one more type of low-hanging fruit: passwords. Many people use the same password for every account out of convenience, but this can be dangerous. Passwords can be hacked, especially when criminals target the victim with programs that are designed to simply rattle through possible passwords until they find the right one. There are programs, such as two-step authentication, that help prevent this, but just having the right password can make a huge difference.

Employees should be encouraged to use a different password for each account, and they should also be taught to create passwords that a hacker would be hard-pressed to guess. Longer passwords with a combination of letters, numbers, and special characters are typically the toughest to crack.

Figure 2: Educational Material for Creating a Password


And the Password is ....
Need Help Creating a Password?
Let's Play A Game!
Think of something, really anything
Is it your pet's name?
No
Yes
Is it one of your names, your kids' or your spouse's names
Start Again
Yes
Does it contain the name of the season we're currently in?
No
Yes
No
start again
No
Does it contain numbers related to your birthday or anniversary?
Yes
Does it contain any variation of the word AmTrust?
Yes
START AGAIN
No
Yes
Is it a password you use for other accounts, personal or work related?
No
Ok…maybe this password has some potential… Wait…it doesn't contain the word PASSWORD right?

Choosing a weak password is a weak practice. Secure yourself and your accounts by observing and following best practices for all your passwords for both work and personal accounts.

Your role is key in securing your company!

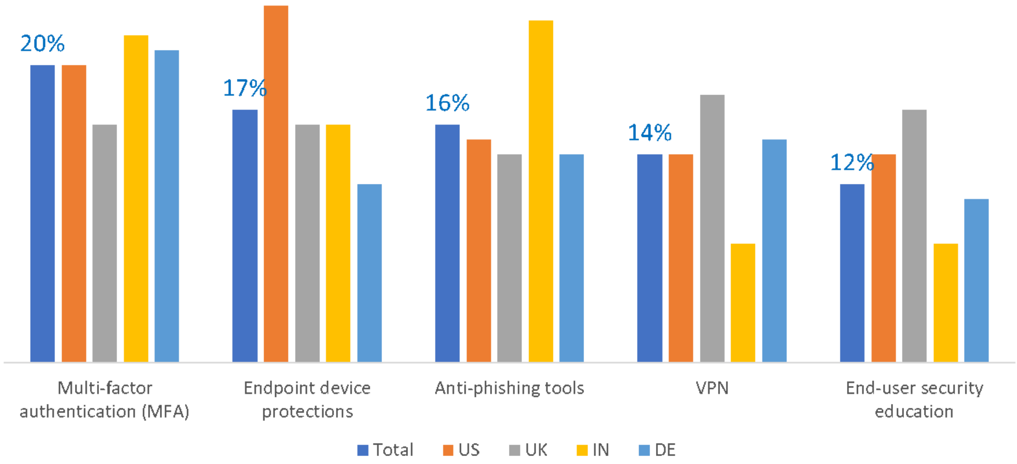
Source: AmTrust Financial

Predict, Prevent, Persist

The unfortunate truth is that no one is completely safe from cybercrime. For as long as the world is connected to the internet, the risk will remain—and even companies that do everything right can be breached. As such, PSPs should prepare for the inevitable. The damage of an attack can be greatly minimized with some advanced planning. This requires predicting what the cybercriminals are after—specifically what data they want and what techniques they might try to get it. Once companies have an idea of this, they can place extra cybersecurity precautions around said data, making it tougher to access. This information should also be periodically checked to ensure that no unforeseen changes/alterations have been made.

Cybersecurity strategies should also evolve because cybercrime is evolving. Phishing is not the only type of attack that is growing more sophisticated. DDoS and ransomware are on the rise. PSPs should educate themselves on the different types of cyberattacks and ensure that they are prepared to counter any attack that might be used against them.

Figure 3: Cybersecurity Investments Since the Beginning of the Pandemic



Source: Microsoft News

Mandatory cybersecurity training should be held for all employees at least once a year to ensure that each link in the chain is strong. Many cyberattacks depend on ignorance to succeed, so continued education is a strong buffer. Businesses that plan for "when" rather than "if" and take appropriate steps to prepare themselves can greatly reduce the risk of cyberattacks in 2021 and beyond.

Opinion

opinion

Cybersecurity affects every company with an internet connection. Everyone has some kind of private data that criminals want, and this information must be guarded to prevent financial and societal damage. COVID-19 has greatly accelerated the move to digital and online business, and Keypoint Intelligence believes that the full fallout of this rapid shift will soon be felt. Not every cyberattack is set to activate right away; some can lie dormant for years waiting for the right event or trigger to activate. Judging by the sheer number of data breaches in the past year alone, the effects will likely be felt for years to come.

Budgets might be tight as we work to emerge from the pandemic, but it is still important for printing companies to take precautions to prevent cyberattacks. Low-cost educational initiatives can help save PSPs from financial ruin, making them well worth the investment.

author

Colin McMahon

Sr. Editorial Analyst

+1 781-616-2100

✉ in

Colin McMahon is a Senior Editorial Analyst at Keypoint Intelligence. He primarily supports the Business Development Strategies and Customer Communications consulting services. He helps to create or refine Keypoint Intelligence's podcasts, industry analyses, and blogs. He also assists with the editing and formatting process for many types of deliverables.

Comments or Questions?

This material is prepared specifically for clients of Keypoint Intelligence. The opinions expressed represent our interpretation and analysis of information generally available to the public or released by responsible individuals in the subject companies. We believe that the sources of information on which our material is based are reliable and we have applied our best professional judgment to the data obtained.