SIM2K
Adapting Technology to Your Business Needs

1•22
Information you can use

SIMformation

Cybersecurity Predictions for 2022

The recent onslaught of attacks, network vulnerabilities, and new compliance regimes means security experts will have their work cut out for them as they enter 2022. *CSO* magazine has collected insights from analyst firms and industry experts to arrive at a list of top cybersecurity predictions for the year.

1. Companies to prioritize supply chain resiliency, responsible sourcing
Threat actors are progressively targeting smaller vendors and suppliers, making supply chain, or third-party, breaches almost inevitable. There have been a growing number of reports of third-party incidents plaguing firms. "60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements," according to a Gartner prediction report. Before onboarding new suppliers or renewing contracts, companies will demand agreement on policies stipulating that their vendors will assume the risk of third-party attacks, paying for costs of remediation, the report suggests.

2. Privacy legislation will accelerate globally
Modern privacy laws could be expected to cover the personal information of 75% of the worldwide population, according to the Gartner prediction report. "The sheer scope of laws like GDPR, and CCPA [the California Consumer Privacy Act] suggests that compliance officers will be managing multiple data protection legislation in various jurisdictions, and customers will want to know what kind of data is being collected and how it's being used," said the Gartner prediction report. The flexibility of an organization's IT architecture will become even more important as new privacy regulations are passed and enforced, regardless of corporate size.

3. Hiring of resident compliance officers will pick up
As organizations face new regulations, there will be a demand for resident compliance officers to help navigate through the complex and evolving dictates. Regulatory bodies will look for a single point of contact for enforcement of policies, thus making it important for companies to designate a person responsible for compliance issues.

4. Bossware will affect employee engagement and insider threats
With a major chunk of the global workforce forced to work from home by the pandemic, there is an upsurge in the usage of software that allows supervisors to monitor employees at all times. This has upset the remote working ecosystem to some extent, escalating employee distress. "Tattleware (also bossware) will degrade employee experience by 5% and increase insider threats in 2022," according to a security prediction report by Forrester. This, according to the report, may also lead to CISOs overcorrecting by reducing the scope of insider threat programs, thereby increasing risks.

5. Security products, supplier management will be consolidated
With major business processes moving to complex cloud environments, there will be a push on the part of enterprises to streamline management of security product suppliers. According to the Gartner prediction report, enterprises will look to adopt cloud delivered secure web gateways, cloud access security brokers, zero trust network access and firewall as a service capabilities from the same vendor. Vendors themselves will consolidate features formerly found in separate applications.

6. Spending on threat detection and response to grow
As significant malware campaigns – including ransomware, spearphishing, and sideloading attacks – proliferated in 2021, information security officials started focusing on getting ahead of cyberattackers in order to protect their businesses. For 2022, security experts expect that the many high-profile and far-reaching attacks in 2021 will drive further spending in threat detection and response.

7. Cyberinsurance premiums will increase
Cyberinsurance will be more expensive, with premiums shooting up, in the wake of recent high-profile cyberattacks. Insurance is like a double-edged sword: While it provides security coverage and has become a "must-have" for organizations, it has also alerted the attackers to asking for even more ransom in the attacks, knowing it is often covered by the insurance carrier. Thus, insurers, hurting from the losses assumed from old policies, are increasing prices by 25%-27% on average going into 2022.

8. Use of CDT (customer data tokens) and BAT (basic attention tokens) to rise
Several experts have been predicting the launch of blockchain-enabled tokens as compensation to security-conscious customers for gathering and using their data. "In the coming few years, 25% of the Fortune Global 500 will employ blockchain-enabled CDT and BAT to compensate their customers," according to a report by IDC. "The idea of compensating visitors/customers with tokens for their time, data, or mere attention has long been an attractive concept to marketers who keep watching the impact and outcomes of their media investments," said one industry expert, citing Brave, an open-source web browser. Brave encourages users to turn on optional ads in exchange for BATs as a reward for their attention to the generated content. Users may pass their tokens to publishers as a way to support selected sites or retain them to, for example, exchange them for premium content.

Whether these predictions all come true in 2022 (number 8 may be the furthest reach of them all) it is an indicator of what we can expect to see developing in the next year and in the future. SIM2K can help you address any cybersecurity concerns you may have or questions about the predicted 2022 trends as discussed.

Log4j Continues to Be Issue

The string of vulnerabilities found over the past few weeks in the widely used Log4j open-source Java component continue to keep enterprise security teams busy. While patching the impacted library should be the priority, identifying all affected applications and servers on big networks is not straightforward due to indirect software dependencies and third-party products.

The problem is the more time it takes organizations to find potentially exposed assets, the more time attackers have to find them and exploit them. Different groups of attackers are currently exploiting the remote code execution flaws, ranging from state-sponsored cyberespionage actors to ransomware groups and cryptocurrency mining and DDoS botnets.
The security community has developed and released multiple open-source tools that can be used to scan directories and file systems for instances of vulnerable Log4j packages, and commercial vulnerability scanners have also added detection for this vulnerability. However, all scanners can have blindspots and that's particularly true when dealing with Java components like lLog4j.

First, while many Java packages come packaged as JAR (Java ARchive) files, this is not the only format used for Java application deployment. Packages called Uber JARs or Fat JARs contain Java programs and all their dependencies, but can be shaded, unshaded or nested. A nested JAR contains other JARs and it can go several levels deep.

This means that a vulnerability scanner with support for Log4j flaws needs to have support for all these application formats and nesting. Simply scanning a directory for JARs with Log4j in their names can miss a lot of instances. According to an analysis by researchers at Google, as of December 19 there are over 17,000 packages on the Maven Central Repository of Java components that depend on Log4j and only 25% of them have released a fixed version. This means the flaw directly impacted nearly 4% of the ecosystem, but 80% of those packages are impacted as a result of indirect dependencies, which means they don't have Log4j listed as a direct dependency. Instead they depend on other packages that pull in Log4j and, according to Google, for a majority of them, this goes five or more levels deep.

Many automated attacks will indiscriminately try to exploit all Java applications, whether or not they actually use Log4j, and this is another example where attacking is much easier than defending. Defenders will have to follow up exploit detections with deeper forensic investigations into whether the targeted applications actually use Log4j or not. If those apps have previously been cleared, they should be checked again with additional scanners because Log4j might be present as a transient dependency or in a nested JAR.

Our major applications are not affected and we have reviewed client systems and passed along vendor correspondence (for instance, SIM2K is aware of 2 client applications that are affected). We are beginning to proactively deep scan systems as a courtesy and will inform you of any findings.

Do You Back Up your Data?

Backing up is the act of making a copy or copies of a file. These files are stored somewhere other than where the originals are located. You may only need to back up a few files, or it might be a much bigger effort. Requirements may differ greatly depending on if you're an individual or a business. The idea is that if the original file is damaged, breaks, is stolen, or suffers any other problem, then the backups survive the issue.

In an age of ransomware attacks, it's crucial to back up data and essential systems. Ransomware authors have been attacking anything from infrastructure to medical systems, leading to potentially life threatening delays and scheduled operation setbacks.

Backing up a device can mean a few things and depending on the device, you may have to be very specific when you map out this process. Sometimes, this can just mean backing up certain mobile settings and functions, or options and data settings for a PC. It can also mean simply copying everything from a particular piece of equipment, as opposed to a few files or folders. This is very common for all forms of mobile devices and laptops. Backing up the entirety of a desktop PC is often a bit more involved due to the sheer number of files. With smartphones, the primary concern is often the vast collection of precious photographs they contain.

One of the most important backup stumbling blocks is figuring out where to place the files being copied. This can be done locally, on an external hard drive or local server on your network. The files can also be saved in the cloud. This can cause a few headaches depending on the security practices of the cloud storage system you're using and whether you encrypt the files and folders before you upload them. If the files are work related, you should be using the business approved storage / backup solution. Placing files in a randomly selected service of your choice can have disastrous consequences if sensitive files are hacked or leaked.

It is important to have "sensible" backups. If an organization simply copies hundreds of thousands of files into a big folder and thinks "job done", that's going to be a problem. If they suffer a ransomware attack 6 months later, the files will be six months out of date and you'll lose six months of work.

The best starting point for most businesses is the 3-2-1 backup strategy, in which you keep three copies of your data, in total.
Two copies of your data on-site, but on different devices.
One remote copy, in case your premises become damaged.
The local copies of your data give you easy and immediate, redundant access to your data when you need it. The remote copy, which will be harder to access, is your insurance policy against fire, flood, and other disasters. To act as a fallback if you are attacked with ransomware, the off-site copy of your data should be inaccessible to an attacker on your network with administrator rights. SIM2K can help you develop a backup strategy and offers off-site storage for remote copies of data. Our Backup Backstop service helps identify critical files and their locations, ensures backups are being made, and also ensures they can be restored.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Want to Roll Back Windows 11?

Congratulations, you got a new Windows 11 computer over the holidays, opened it up, and turned it on. And, now you miss being able to right-mouse-click on the taskbar, or pin things on the taskbar, or doing any number of things you've been doing since Windows XP.

So, do you want to stay on Windows 11 or install Windows 10 on that new computer. Hopefully you have enough RAM (16GB or more), a processor that can support Windows 11 (even if you don't want to install it), and more importantly, an SSD drive. If you have a computer that doesn't have an SSD, you may see something like Costco warned about on its website: "After the initial boot up of your laptop, your device may experience performance lags for approximately the first one to two hours as performance features are downloaded and installed. The laptop will return to normal operating conditions once all downloads are completed." That's certainly not the best experience with a new laptop, and a sign Windows should not be deployed on systems with old-fashioned hard drives. If you still have a Windows 10 machine using an older hard drive, figure out whether you can upgrade to an SSD.

Before you think about installing or downgrading to Windows 10, consider first the third-party software that can bring back many of the features you want. There are many options to choose from, including Startallback and Start11. Both bring back many of the traditional menu functions Windows 10 users want. Tech experts suggest you install either one first and see whether Windows 11 is acceptable with these additions.

The question then is whether users can downgrade to Windows 10 if the machine is running Windows 11. A Windows 11 license is a digital one that allows an install of Windows 10 on a machine running 11. But, as a Lenovo support note points out, a clean install of Windows 10 may require that you download needed drivers. If you're lucky, as the machine gets online and checks in online, the drivers will trickle down in the background and get installed. If not, you will need to search for what is needed. Get them from a vendor' site, do not download drivers from a random driver site, as more often than not they will include malware.

Bottom line, if you have a Windows 11 computer now and want to run Windows 10, IT experts recommend that you first try third-party tools to make it look and act like Windows 10. Reinstalling a clean version of Windows 10 can be easy – or an absolute annoyance if you can't find the right drives for full functionality.

If you are a more advanced user and still want to downgrade, the pros suggest getting a backup program to fully image your Windows 11 system as it was when shipped, then attempt a clean install of Windows 10. If you can't find all of the drivers you need, you can always roll yourself back to what was installed on the computer. Just ensure that you know your options before deciding you don't like Windows 11. We will be glad to discuss options for you – call us.

"Random Tid-Bytes"

Phishing Takes Many Forms – all Bad

There are many types of phishing attack nowadays, to the extent it can be tricky to keep up with them all. Here is an explanation of the three major phishing terms:

Phishing attack

Think of this as the main umbrella term for all phishing attempts. It doesn't matter if it's a spear, a whale, a smish (text attack) or a vish (voice mail message). This is where someone tries to have you login on an imitation website. This site may emulate your bank, or a utility service, or even some form of parcel delivery.

Spear phishing

Regular phishing attacks are blasted out to random recipients in their hundreds, thousands, or hundreds of thousands. Spear phishing, by contrast, is targeted at specific people, often obtained from your company website or LinkedIn postings.

Whaling

Whaling is the gold standard for targeted phish. They're the biggest and most valuable people or organizations to go after. "Whales" are typically CEOs or other people crucial to the running of a business. They'll have access to funds or be deeply embedded in payment processes/authorisation. CEO/CFO fraud, where scammers convince employees that the CEO/CFO needs large sums of money wired overseas, is common. This is also more broadly known as a business e-mail compromise scam.

SIM2K offers training to help your employees recognize phishing attacks and how to protect your data from unauthorized access. Call us for more information.

Zultys Introduces New Phone for 2022

Zultys, our unified communications partner, is adding the new 47GE as the flagship tier phone to kickstart 2022. "Absolutely loaded with features," as Zultys says, the ZIP 47GE boasts a hi-resolution color display, dual Gigabit Ethernet ports, 27 programmable soft keys, a dedicated headset port, and Electronic Hook Switch support to offer enhanced usability for wired and wireless headset users. The optional ZIP 450M Expansion Module supports up to 180 additional programmable soft keys. The ZIP 47GE is fully compatible with Zultys' ZAC Unified Communication and Collaboration solution, allowing users to manage calls and messages directly from their computer. It also works seamlessly with the Session Initiation Protocol (SIP) open standard, managed from the Zultys MX Administrator application for rapid deployment and the industry's lowest total cost of ownership. This feature-rich IP phone is ideal for executives, while its soft key expandability also makes it ideal for operators and receptionists. If you want to upgrade your desktop phone, call SIM2K for more information or to order a Zip 47GE for your office!

What will 2022 Mean for the Office?

The workplace has changed significantly in the past couple of years, and there's unlikely to be any letup this year. The COVID-19 pandemic has already shaken up perceptions and expectations of what work should be, and most employees now expect greater flexibility over where and when they do their jobs. Adapting to a hybrid remote work strategy will continue to be a focus for many businesses in 2022.

Support for flexible work is just one of the ways companies may seek to retain staff amidst a wave of resignations across a variety of industries — another trend that's likely to impact businesses and influence strategies around technology investments.

Here are some of the ups and downs tech industry analysts envision for the year ahead.

Hybrid work to dominate as offices reopen, but many efforts will 'fail' at first

For many organizations, any long-term strategy around remote work remains a work in progress, but surveys indicate that some level of remote work will continue post-pandemic. This is good news for workers, who reap the benefits of an improved work-life balance, and for employers, with surveys indicating an increase in productivity with remote workers.

A successful hybrid work strategy bridges both physical and virtual communication to connect employees no matter where they are located. That's the overarching goal, at least; actually achieving this will be a challenge, according to Forrester.

The analyst firm predicts that around 10% of companies will go entirely remote post-pandemic, while 30% will opt for fully in-office. The remaining 60% will take a hybrid approach. And of those that adopt hybrid work, a third will fail — at least in the first attempt, Forrester said in its report 'Predictions 2022: The Future Of Work.' "Of the three possible paths – back to the office, hybrid, and fully remote – hybrid is the most challenging," said a Forrester analyist.

Why is hybrid work so problematic? While most companies now have almost two years' experience handling a fully remote workforce – on top of many years' experience working in the office – hybrid work is more of an unknown. Combining the two conflicting modes of working creates its own challenges. Many organizations have supported distributed teams or have had a handful of fully remote workers in the past. But nothing has prepared the entire organization to learn how to be in the office two to three days a week.

The strategy raises new questions, such as who should be in the office on which days and for what purpose which are things companies are ill-prepared to answer. The experiments companies will have to undergo to figure that out may take an entire year to sort through, assuming companies and corporate leaders have the patience and cultural flexibility to do so. Those that do not can be expected to revert to all-office or all-remote polices mid-year, Forrester predicts.

Invasive monitoring tools to spur employee backlash, prompt legal action

With remote work likely to remain in some form, businesses will need to consider how they track worker productivity and well-being when physically removed from staff.

Business interest in "bossware" style software that provides detailed analytics on employee actions has grown during the COVID-19 pandemic, drawing criticism from worker rights groups as overly intrusive. These tools can include regular screenshots of an employee's laptop or keystroke-logging to track productivity levels. Depending on how they are implemented, such tools can seriously undermine trust, particularly when used without employee consultation.

It's not only bossware tools that have raised concerns. The tech industry more generally is still figuring out how to balance the benefits of workplace data analytics with the need for worker privacy. For instance, the introduction of Microsoft's Productivity Score last year drew controversy over its inclusion of individual employees' data; Microsoft later took steps to ensure data was anonymized more effectively.

Major collaboration and productivity vendors are treading carefully around employee privacy concerns. But individual organizations will have to ensure they don't overstep employee privacy laws – and employee perceptions – of how much monitoring is acceptable. If employers get it wrong, at best, this risks damaging employee trust, and at worst it could see employees suing for unfair dismissal as a result of the way these tracking tools are used. Therefore, businesses should carefully consider what they are tracking and why, and whether direct monitoring is even necessary or performance can be tracked in a less intrusive way.

Staff shortages to prompt improved employee experience

One of the major workplace trends of the past year was the rise of staffing shortages across a number of industries, part of the so-called "Great Resignation." The situation is likely to continue into 2022, with employers struggling to hire the right staff – and investing to keep hold of those already employed.

This is expected to lead businesses to focus on three areas:

- Employee sentiment analysis to ensure there's no imminent exodus of employees, and to address problems as they arise;
- Improved internal communication and employee engagement;
- Investment in learning and development programs to give people the opportunity to develop their career – either on the same career path or in a completely new direction – without leaving the organization.

One way to retain staff will be to allow flexibility at work: organizations that decide to go back to a fully on-site arrangement could lose up to 39% of their workforce, according to the 2021 Gartner Hybrid Work Employee Survey. Forrester also predicts that concerns about employee retention will drive a "surge of spending" on "employee-centric initiatives and technologies" during 2022. This will lead to 20% of HR budgets being allocated to employee experience initiatives, while the number of organizations with a formal employee experience program in place will rise from 48% to 65% in 2022. Employee recognition budgets will also go up, from 1% of total compensation to as high as 2%, Forrester predicts.

Ultimately, it's about creating a culture where workers feel valued and connected to the rest of the organization. Whatever path your company may take as the variants of Covid-19 race through the workplace, SIM2K is prepared to support you in-office, remotely or the hybrid mix.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com