Raising Customer Awareness of Cybersecurity

By Joseph Saracino

Cyber threats are more pervasive than ever and growing. Check Point Software's Cyber Attack Trends: 2022 Mid-Year Report noted that cyberattacks intensified by 42% in the first half of 2022. Cybercrimes in the United States alone were responsible for over $4 billion in losses in 2022, according to the Federal Bureau of Investigation.

Even with this staggering data, many companies have failed to recognize just how serious and widespread cyberattacks are and their far-reaching ramifications. Beyond the loss of proprietary company data, there is the compromise of customers' and employees' sensitive personal information, productivity losses, costs incurred to remediate a breach, reputational damage, and loss of customer confidence. If an organization is found to have been non-compliant with cybersecurity laws and regulations, hefty fines may also result. For insurance brokers and agents, educating their clients regarding today's perilous cyber landscape and what an effective cybersecurity program consists of, is a way to demonstrate the value-add expected of a trusted advisor.

Today's Cyber Landscape

Following the 1,802 data breach cyberattacks in the U.S. in 2022 as reported by Statista, in which 422.14 million individuals were affected, 2023 continues with growing cyberattacks and new threats. Ransomware attacks remain the number one threat and now we are seeing cybercriminals target entire nations. Cloud supply chain attacks are also on the rise, most notably, those involving open-source communities. Other top cyberattacks projected for 2023 include: mobile device, phishing/spear phishing, crypto jacking, state-sponsored, Internet of Things (IoT), social engineering/social media, smart medical device, cyber-physical/infrastructure, and denial of service attacks. Further increasing our vulnerability to cyberattacks are today's hybrid and remote working environments.

Where most organizations remain most vulnerable is in their lack of endpoint protection. An endpoint is any physical or virtual device that is connected to an organization's Information Technology (IT) network (e.g., PCs, laptops, tablets, mobile phones, routers, and printers). With more people working remotely or in a hybrid model, the number of endpoints has significantly increased. Open ports, created by unpatched software, misconfigured applications, and weak credentials, also increase an organization's likelihood of experiencing a cyberattack.

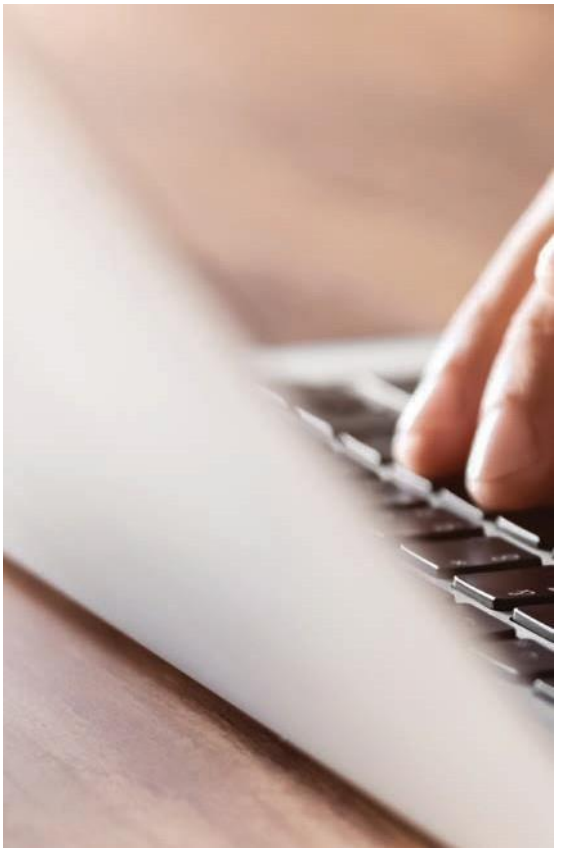
New Technologies and Threats

Cyber criminals are also gaining ground in their nefarious deeds by relying on new technologies. One example is the "post-exploitation framework" designed to secretly deploy ransomware within enterprises. The framework, EXFILTRATOR-22 (EX-220), is capable of establishing a reverse shell with elevated privileges, uploading/downloading files, logging keystrokes, and launching ransomware to encrypt files. It can also start live Virtual Network Computing (VNC) sessions through which criminals can gain real-time access to the network.

iPhone users are at risk for a new cyber threat, which police stations nationwide are reporting. Cyber criminals are exploiting the iPhone's passcode feature by observing users tap their passcodes, which are usually just several digits. Then, they apply that information to access their devices. Once they have access, they change the passcode associated with the iPhone's owner, who is then locked out of their account, including all information stored on the iCloud. Cyber criminals can then gain access to the owner's financial accounts, health records, and other personal information.

In addition to the iPhone platform, another example of a platform being targeted with cyberattacks is Microsoft Office Outlook. These attacks include privilege escalation and remote code execution vulnerability exploitations. In privilege escalation attacks, criminals obtain users' authentication credentials without any user interaction and then send malicious messages that trigger an authentication request enabling them to access sensitive information and systems. Remote code attacks enable criminals to execute arbitrary code with the victim's privileges to gain remote access to the system.

What's further intensifying cyber threats is the speed at which they are now occurring. Rapid7's 2022 Vulnerability Intelligence Report cited that the time it takes from when a system vulnerability is disclosed and when a cyberattack takes place is decreasing. It's typically a period of seven days, representing a 12% and 87% increase in the exploitation speed



timeframe in 2021 and 2020, respectively. Given today's cybercrime environment and increased threats, federal and state governments are stepping up their efforts to fight cybercrimes.

Government Actions

For many years now, federal and state governments have taken measures to protect sensitive personal information. Numerous laws and industry standards have been enacted for this purpose. Among them are:

The Health Insurance Portability and Accountability Act (HIPPA) designed to ensure that ensures the confidentiality, availability, and integrity of personal health information (PHI).

Payment Card Industry Data Security Standard (PCI DSS) encompassing various regulatory standards intended to ensure that all organizations maintain a secure environment for credit card information.

New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCCR 500), a regulation introduced by the New York State Department of Financial Services which establishes cybersecurity requirements for financial service providers.

System and Organization Control 2 (SOC 2) SOC 2, a voluntary compliance standard for service organizations developed by the American Institute of CPAs (AICPA) which specifies how organizations should manage customer data.

The General Data Protection Regulation (GDPR), a regulation of the European Union (EU) which sets forth standards for organizations located in or outside of the EU that collect data or target individuals in the EU.

The Federal Educational Rights and Privacy Act (FERPA), a U.S. federal law designed to ensure that students' educational records are protected and private, which applies to all educational institutions that receive funding from the U.S. Department of Education (DOE).

The National Institute of Standards and Technology (NIST), which promotes innovation, industry competitiveness and quality of life with the advancements of standards and technology, and which has issued the NIST 800-53 Risk Management Framework providing guidelines to support and manage information security systems, and the NIST 800-161 Supply Chain Risk Management Framework.

The California Consumer Privacy Act (CCPA), a California law developed to provide consumers more control over the data that organizations collect about them.

Cybersecurity Maturity Model Certification (CCMC), which imposes stringent cybersecurity measures on certain organizations that handle controlled unclassified information and to safeguard sensitive information.

New York Shield Act, which strengthened New York's prior 2005 Information Security Breach and Notification Act by expanding the types of private information companies must provide consumer notice of if a data breach occurs.

More recently, the Biden Administration unveiled its U.S. National Cybersecurity Strategy, developed by the Office of the National Cyber Director. Already under-

continued from page 41

way, this plan is introducing more aggressive liabilities for "those entities that fail to take reasonable precautions to secure their software." In addition, the new strategy authorizes law enforcement and intelligence agencies to hack into the networks of foreign entities to prevent cyberattacks or retaliation against advanced persistent threat (APT) campaigns. This strategy is intended to serve as a preemptive strike using "disrupt and dismantle" tactics against hostile networks of cybercriminals and adversarial foreign governments and disabling perceived threats to national security or public safety.

Insurance Carriers

Given the high cost of cyber breach claims, insurance companies are taking a much harder look at potential cybersecurity insurance policy holders. NetDiligence's Cyber Claims Study 2021, which reviewed cyber incidents occurring between 2016 and 2020, found the average cost to an insurer for a small and medium sized enterprises breach is $145,000. For large companies, the average costs can rise to $10 million.

With these high-cost claims, insurers are establishing baseline criteria, which they expect organizations to meet before they will consider issuing a cybersecurity policy. They include a proactive and consistent approach to managing cyber risks: multifactor authentication (MFA); comprehensive backup; regular penetration testing and vulnerability assessments; patching; cyber awareness training for employees; and incident response plan.

Cybersecurity insurers want to know that an organization is fully committed to cybersecurity and has taken the appropriate steps towards mitigating their risks.

The Role of Insurance Advisors

Brokers can perform a real value-added service to their clients by raising their awareness of the importance of establishing a sound cybersecurity program. Taking a consultative approach, they can start by asking key questions such as:

- Are you operating a hybrid IT infrastructure (on-premises and in the cloud)?
- Are you using common access interfaces (e.g., PowerShell, PsExec, MSI, etc.)?
- Are you using technologies such as multifactor authentication (MFA) and agentless and proxy less technologies to extend MFA, as well as risk engines that continuously assess IT system usage?
- Are you triaging MFA requests and using an escalation policy for managing high-risk situations?
- Do you currently have a comprehensive cybersecurity program in place that includes regular penetration testing (ethical hacking), vulnerability assessments, employee cybersecurity education and training, established cybersecurity policies, and an incident response plan?

Once a client's situation has been assessed, insurance professionals should see where they stand in terms of qualifying for a cybersecurity policy. If security measures need to be taken, the client should be encouraged to promptly follow through with the appropriate actions. This is where partnering with a dedicated cybersecurity firm is important.

Many companies believe that their managed service provider and/or their internal IT team are qualified to manage the cybersecurity function. But unless those individuals have the essential credentials (e.g., Certified in Risk & Information Systems, Certified Network Security Administrator, Computer Hacking Forensic Investigator, Certified Information Security Systems Auditor, Certified Information Systems Security Professional, Licensed Penetration Tester, Systems Security Certified Practitioner, Certified Security Analyst, etc.) and experience providing cybersecurity services, they are not qualified. And, as the individuals tasked with overseeing IT operations, they are not an objective third-party, which is important to regulators should a breach occur.

Cybersecurity Partners

When looking for cybersecurity partners, insurance professionals should seek a firm that is not simply a vendor of technologies and services. In addition to having a proven track record and qualified, credentialed staff, the firm should exhibit a level of cybersecurity expertise and serve its clients in an advisory role and not in a transactional role. They should be proactive in supporting an organization's ongoing cybersecurity. That means keeping both their insurance partners, as well as their mutual clients, advised of the latest threats and developments, taking a role in educating and training the client's employees, and developing a program tailored to the client's specific industry, size and threat potential, in addition to supporting their regulatory compliance. The right cybersecurity partner will assume a long-term risk management strategy and not short-term technology fixes. Reporting to an organization's C-level suite, a cybersecurity partner becomes a trusted advisor in the same way that insurance professionals are to their clients.

By teaming up with the right cybersecurity partner, insurance professionals will become more proficient in cybersecurity, gaining broader knowledge and in turn, becoming a better resource and advocate for their clients especially when a cyberattack occurs and a claim must be filed.

Cause for Optimism

Damages stemming from cybercrimes are projected to reach $10.5 trillion annually by 2025 according to Cybersecurity Ventures. There is, however, some cause to be optimistic as more organizations recognize that cybersecurity must become embedded in their broader corporate culture. In fact, Gartner analysts reported that by 2026, at least 50% of C-level executives will have performance requirements related to cybersecurity risk built into their employment contracts. Further, according to Gartner by 2025 60% of organizations will use cybersecurity risk as a significant determinant when conducting third-party transactions and business engagements.

The tide is turning, and insurance professionals can ride the wave to strong client relationships by taking a proactive and advisory role in the critical area of cybersecurity.

Saracino is president and CEO of Cino Security Solutions.