In Their Own Words…
How Accountants Can Help Protect You from Cybersecurity Threats

By Gundi Jeffrey, Managing Editor

Gundi Jeffrey, Managing Editor of ThinkTWENTY20, is an award-winning business journalist specializing in writing about the accounting profession for various publications in Canada and England.

Our businesses and organizations are bombarded with incidents of ransomware, malware, adware, phishing and many other types of scams and cyber attacks. And we use a wide variety of access controls, including SIEM (security information and event management) approaches, firewalls, IDs, IPs, proxies, PKI (public key infrastructure) services and a ton of software programs claiming to protect our networks and IT systems. And yet, one wonders, if there are so many solutions out there and so many expert security advisers, why are there still so many security breaches?

> Organizations should develop a plan for attracting, growing and retaining cybersecurity and privacy talent in an increasingly competitive market.

Accounting firms and specialized boutique consulting firms have stepped into the fray to offer their solutions to the cybersecurity problems plaguing both individuals and companies throughout the world. Between them, they offer a wide range of services, including but not limited to:

- *Pre-breach security assessments*. Includes social engineering and phishing tests, vulnerability tests, penetration testing, web and application testing, security posture assessment against National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO) and other frameworks, the Supervisory Control & Data Acquisition System (SCADA) and embedded tests, as well as the Internet of Things (IoT) security assessments.
- *Strategy, Transformation & Risk*: Developing business-focused strategies and programs that support growth and agility by making cybersecurity, privacy and financial crime an enterprise-wide priority.

- *Compliance Planning*. For audit and assurance engagements.
- *Offensive Security*: Vulnerability assessment, penetration testing, configuration reviews, etc.
- *Implementation & Operations*: Designing, implementing, operating and optimizing the use of cybersecurity, privacy and financial crime technologies.
- *Data Protection*: privacy, incident response management, etc.
- *Digital Forensics*.
- *Crisis Management*: Managing impact to the businesses from emerging threats by identifying, preparing, responding, investigating and remediating threats.
- *Security Implementation and Operations*.

In short, they help plan to make and keep you safe and, if the worst happens, help you recover and plan for the future. What does all this involve? Here's a detailed take three of Canada's accounting firms, as well as one specialized consultant, have on this issue. And, given the multi-faceted impact that Covid 19 has had on the economy and businesses of the entire world, the issue has become even more important in recent months.

ThinkTWENTY20 spoke with Sajith Nair, Partner, Cybersecurity & Privacy, PwC Canada; Vivek Gupta, National Leader, Cybersecurity & Forensic Technology Services, BDO Canada LLP; Blair Brown, Director, Cybersecurity and Compliance, Baker Tilly KDN; and Theresa Azari, the principal consultant of Vancouver-based Veritus Consulting Services. Although the article that follows is long, it is packed with useful, detailed information for just about anyone operating in today's cyber-infused world.

ThinkTwenty20: *What do you consider to be the biggest cybersecurity threats to the majority of your clients?*

Sajith Nair: Based on years of experience doing proactive and reactive work for our clients, there are four main types of cyber threats. The underlying technical methods across these threats are often similar; the key difference is their motivation and what they might target.

- *Nation states* are looking for economic, political or military advantage and, therefore, often target critical infrastructure providers (e.g., banks, utilities, telcos, transportation) or organizations that may hold data of importance to them (e.g., research institutions, governments).
- *Organized criminals* are looking for immediate financial gain so they will target organizations to steal personally identifiable information (customer or employee), extort using ransomware, commit wire transfer frauds, or steal credentials (customer or employee).
- *Hacktivists* are looking to influence political and/or social change, so they specifically target certain businesses or government organizations to embarrass them by stealing data or disrupting business operations.
- *Insiders* are driven by personal advantage, monetary gain, professional revenge and so they either steal data, commit fraud or cause business disruption. Insiders increasingly are also bribed or coerced by the other threat actors listed above to assist them.

Vivek Gupta: I believe that the biggest cyber security threat for any organization is the weakest link in their cyber defence program, the "people" component. Organizations can spend thousands of dollars on the latest and greatest technology to protect their assets but, even with this in place, they are only as secure as their weakest link, their people. Employees/contractors may inadvertently fall victim to cyber attacks by clicking on a link in phishing email, unknowingly disclosing sensitive information, visiting a malicious website, sharing their credentials with others, wiring money to a fraudulent bank account or using personal devices to access and store company data. An inside employee may also become disgruntled (due to lack of promotion, poor performance review, conflicts with management, etc.) and may be motivated to cause harm to their organization.

Blair Brown: Ransomware, directed phishing attacks, malware free attacks and supply chain attacks are continuing to increase. Additionally, a growing concern is the risk presented by internal data leakage. These attacks were on the rise prior to the pandemic, but the risk has only increased with the distribution of the workforce and the rush to implement telecommuting options. This risk is particularly high among smaller clients who have limited IT resources. We identified these as emerging concerns and have been very proactive in advising clients on how to manage these risks.

Theresa Azari: The way I see it, social engineering and third-party vulnerabilities (especially in the cloud) are huge concerns for my clients.

ThinkTWENTY20: *And would those be the same type of threats you, as an accounting, auditing and consulting firm would face? Or are there different threats for your type of business?*

Nair: As one of the world's largest professional services companies, we face similar types of threats as those of our clients globally as we become an extended part of their business ecosystem.

Gupta: Our assets, services, sensitive data and technology may differ from other organizations such as a manufacturing or utilities company; however, we face similar threats, such as denial of service attacks (causing service disruption), data breach or compromise, ransomware and insider threats, to name a few. What does differ from business to business are the financial, operational and reputational impacts of a successful cyber attack. For example, if a power generation company gets hit with a cyberattack, it could have severe consequences for employee safety, as well as leaving thousands without heat/electricity, and numerous other legal and regulatory ramifications.

> When more employees are working remotely from home, we need to be mindful about extending good security practices beyond the traditional corporate infrastructure.

Brown: As an organization, we face the same threat spectrum as our clients and we remain sensitive to the risk. As we have seen with the recent security incidents at MNP and Desjardin, firms in this sector are targets.

Theresa Azari: Yes, they are the same. Despite the different line of business, we have access to highly sensitive data that cyber criminals want to steal.

ThinkTWENTY20: *Can you offer an example or two of a client's (unnamed of course) data hack or a malicious cyberattack and the resulting damage caused?*

Nair: We have seen all kinds of breaches relating to the four most common types of threats discussed above. The top three reasons for the breaches in most cases were:

- *Bad technology hygiene***.** This includes an attacker exploiting unpatched systems, legacy systems, poorly designed applications and networks, or unmanaged assets.

- *Weak credential management*. This includes an attacker using weak credentials to gain access to systems due to failure to use multifactor authentication, insufficient password controls and a lack of ongoing automated rotation of cryptographic keys, passwords and certificates.
- *Human factor*. This includes an attacker bribing or coercing an insider to willingly assist them or tricking an insider (e.g. phishing) to unwittingly assist with a breach.

The damage to our clients in each case has ranged from financial loss, brand damage, employee morale and productivity issues, missed business opportunities, regulatory penalties to, in very extreme cases, legal actions.

***Gupta*:** We do have some clients that have reached out to us in a state of panic because they fell prey to a ransomware attack. The stories are usually the same: an unsuspecting employee opens an attachment received from a legitimate looking sender (usually impersonating someone in a position of authority) and their systems are instantly encrypted. A hacker is demanding payment or “ransom” to allow access to be regained and they don’t know what to do. Depending on their incident response or backup and recovery strategies, they may not be able to successfully restore production systems, resulting in data loss and the inability to provide services to their customers. In some cases, organizations have to resort to using paper files until their systems can be re-built. The financial, reputational and operational implications of such attacks can be significant.

***Brown*:** In one case, we were asked to help assess why a large law firm was facing a constant barrage of external attacks, despite having an extremely strong intrusion prevention and detection system (IPS) and enhanced perimeter defences. They kept getting attacked and the attack vectors and type of attacks kept changing in an extremely rapid manner – as soon as one type and manner of attack was detected using their defence systems, the attack would morph and change. Occasionally, there would be multiple attacks.

The level and sophistication of the attacks pointed to a rogue state actor. After consultations with the RCMP, we collectively realized it was a state actor. We traced the start of the attacks to a specific time frame and, after a thorough internal and external forensic analysis of events at the start, we realized that one of the leading partners at the firm was engaged with a client that had a string of litigation proceedings against a powerful figure in a state government. Once that was brought to the attention of the managing partner, the firm removed itself from dealings with the client and the attacks stopped.

Why, if there are so many solutions out there and so many expert security advisers, are there still so many security breaches?

The level, speed and sophistication of the attacks was unlike anything we or the RCMP cyber team had experienced before. We are thankful that such types of attacks are extremely uncommon, but they can lead to a lot of disruption, loss of earnings and major reputation damage.

More directly related to the COVID crisis, we recently had a situation within a company where a senior executive's account password was compromised through an attack against a social media application. Two-factor authentication was enabled on the company's sensitive systems, but not on the email account (since corrected).

The attacker used the credentials to gain access to email and create directed and highly plausible emails to financial staff directing a transfer of funds to an overseas account. Fortunately, this occurred as staff were beginning to work on site and were not working remotely due to COVID. We were alerted immediately and traced the email chain, identified the scope and were able to lock down affected accounts before the funds were transferred or any other action could occur.

Theresa Azari: One of my clients was recently the victim of a social engineering attack. The cyber criminals managed to obtain access to PII data due to a vulnerability in the environment. This enabled them to impersonate an authorized source, in an attempt to transfer funds to another destination.

ThinkTWENTY20: *What are the most common steps your clients should take to protect themselves? Are you seeing good security strategies?*

Nair: We are seeing our progressive clients take a combination of strategies:

- *Adopt a comprehensive cyber risk management program.* The program should address specific risks and digital crown jewels for the business, identify how management keeps current with new threats and include a tested cyber-incident response plan that contains robust communication and brand-management protocols.
- *Grow through secure digital transformation.* Many organizations are transforming their business model by using emerging technologies (e.g., artificial intelligence, industrial systems, robotics, Internet of Things and 5G) to develop new products or automate their operations. It's important to understand the new threats and vulnerabilities this will introduce and design transformation strategies with security in mind from the start.
- *Use data with confidence.* Growing privacy regulations are creating doubts as organizations use data, resulting in missed business opportunities or regulatory breaches. Organizations that integrate privacy and data ethics as core principles in their enterprise data strategy and governance can use data with confidence to create new opportunities.
- *Unite your lines of defense.* As security, financial crime, safety, reliability, privacy and data ethics become increasingly intertwined, leading organizations are taking a proactive approach to build digital trust. They're integrating their traditionally siloed strategies so they can innovate with speed and confidence.
- *Develop a talent and upskilling plan*. Organizations will need access to the right talent. They should develop a plan for attracting, growing and retaining cybersecurity and privacy talent in an increasingly competitive market. This should include partnerships with academia, industry associations and service providers. Organizations should also upskill their front-line business and technology teams to manage digital risks closer to where they occur, and not rely solely on their cybersecurity and privacy functions.

Gupta: We recommend investing in a strong cyber security training and awareness program that educates employees about the latest cyber security risks and threats on an ongoing basis.

In addition, it is critical to make sure you have the fundamental controls in place. As an example, enforce strong password controls (using Multi-Factor Authentication, when available), apply patching and system updates regularly, know the assets connecting and being used on your network, install anti-virus software, practise the principle of least privilege when providing access, perform regular backups and know your third-party suppliers. Planning is also critical for organizations; Business Continuity, Disaster Recovery and Incident Response Plans should be developed and reviewed/tested to allow the timely response and recovery from a cyber attack or service-impacting incident.

We are seeing various strategies with respect to cyber security depending on the size of the organization. No matter the size of an entity, strong security strategies are closely aligned with business objectives and start with a risk-based approach to identify the likelihood and impact of potential threats and risks. The results allow organizations to prioritize what they protect and how they plan on protecting their critical data, systems, services, using people, processes and technologies.

Brown: We advise our clients on how to achieve compliance, security and risk mitigation through the strategic application of a program of balanced and cost-effective governance and best practice technical controls, such as NIST, COBIT, PCI, etc.

Planning starts from a position of zero trust; this focuses efforts on the controls required to meet operational requirements and access the data most important to the client. By applying controls against endpoints, users, data access, etc. the kill chain of many common attacks can be broken and the client protected. A program is built from this perspective to meet the client needs and effectively mitigate the risk.

Critical to this process are the implementation of an ongoing program of security awareness for all staff and, from a technical perspective, a strong vulnerability management and incident response program.

Theresa Azari**:** Organizations can protect themselves by practising good security hygiene – provide security awareness and role-based training to all personnel (security is everyone's job, not just that of the security folks); routinely scan your network for vulnerabilities and patch them in a timely manner according to CVE severity (know where you have holes and fix them fast); leverage industry frameworks and guidance, such as NIST CSF, CIS Top 20 controls to create, deploy and maintain a robust security program. Security strategies are getting better as senior leaders realize that breaches are accelerating at an unprecedented pace and rigour (it's not a matter of "if," it's a matter of "when").

ThinkTWENTY20: *I have been reading that Covid 19 has ramped up this subject, as it seems to have spawned several new types of risks and threats to corporate cybersecurity. What specifically do we need to look out for?*

Nair: We have seen organizations take several actions to manage the threats in the COVID-19 pandemic environment, including:

- *Additional user awareness* focusing on secure remote working practices, educating staff COVID-19 themed phishing campaigns and scams and targeted awareness for high-risk functions that handle financial transactions or access high volumes of sensitive data.
- *Enhanced insider threat risk management* focusing on administrative users, users with access to large volumes of data and users where historically physical controls were used for data protection (e.g., contact centres).
- *Enhanced technology controls* related to remote access and user endpoints.
- *Enhanced monitoring* focusing on unsanctioned cloud services, critical third parties (suppliers/vendors) and monitoring for COVID-19 themed attack campaigns.
- *Enhanced customer authentication* to digital services (e.g., step-up authentication,

conditional access).

Gupta: The Coronavirus swept across the globe in early 2020 and forced companies to move from an onsite/office working model to a remote/work from home model in order to protect the health and well-being of employees and the general public. Information technology departments were forced to rapidly respond and implement solutions that enabled employees to have the same access (resource, utilities and services) as they did prior to working remotely. A consequence of this rapid shift was that IT departments potentially prioritized connectivity or security and, as a result, existing security protections may have either been bypassed or disabled.

Ordinarily, a shift in operating models would require months of planning but, in this case, organizations did not have this luxury. At the same time, cyber criminals are increasing attacks under the guise of the Coronavirus pandemic. We have seen examples of fraudsters posing as: cleaning companies, charities, financial advisors and government agencies. Although the risks are not new, they are exacerbated by the mental stress people are under because of the pandemic and the fact they may be using home-based networks that do not typically have the same protections as an office environment. Employees may be using personal PCs (shared among other individuals in their household) and mobile devices to access information and perform work functions.

Brown: Many employees are currently working from home networks, which typically tend to be less secure than corporate networks. This has led to an increase in attacks against individual home networks in the hope of compromising the home machine and using that as a launch pad to try to penetrate the corporate network or simply to phish and spoof emails to execute transactions or instructions to transfer value to the hackers' accounts.

The FBI has identified a 400% increase in reported attacks. What we have commonly seen is COVID being used as premise or pretense for these attacks. Examples include:

- Elevated focus on underfunded or under resourced enterprises.
- Elevated phishing attempts with a COVID theme.
- Increased attacks against the public sector and health institutions.
- Increased attacks directed against manufacturing and the supply chain.

Clients need to be very aware of this activity and guard against very directed and plausible campaigns taking advantage of the pandemic and a remote workforce.

***Theresa Azari*:** The shift to working from home has significantly increased cyber risks and an organization's ability to scale up their infrastructure to manage the higher volume and new forms of data flows.

ThinkTWENTY20: *What steps should companies take to protect themselves with employees working at home?*

Nair: We have seen organizations take several actions to manage risks from remote working:

- Ensuring on-premise security controls still apply to systems when staff are not on the internal network.
- Monitoring for shadow IT and moving staff toward approved solutions.
- Ensuring remote access systems are fully patched and securely configured.
- Monitoring remote access systems, email and Active Directory for anomalous logins.
- Monitoring and reacting to issues encountered by staff with remote working.
- Educating and supporting staff to work safely and securely from home.
- Reviewing tactical actions and retrospectively implementing key security controls which may have been overlooked to enable remote working in haste during early days of pandemic.
- Ensuring remote access systems are sufficiently resilient to withstand DDOS attacks.

***Gupta*:** As a starting point, remote access management policies and procedures should be reviewed, updated, and technical protections such as multi factor authentication (MFA), virtual private network (VPN), and internet protocol (IP) restrictions should be implemented. These updates, along with awareness training around the risks, threats and best practices, should be delivered to personnel. Devices used by employees should have the latest patches/updates, and be equipped with end-point protections (anti-virus/malware) and restrictions to prevent unauthorized software installation and the transfer of data. It is also critical that companies understand and review who has access to sensitive or confidential information and that this is performed at the network level to identify any suspicious activities. Employees should also be provided with incident response procedures and contact information for IT support/help desk personnel in the event they need to report an issue or unforeseen event.

Brown: In my opinion, a solid strategy would be for them to engage with their IT staff or managed service provider to implement the best practices outlined in the CIS Basic and Foundational Controls.

If you consider that, as a defender, your objective is to stop the adversary, to break the kill chain, then in many cases some very straightforward and low-cost controls can be highly effective. In addition to a strong security awareness program, simple best practices such as: whitelisting of software to restrict installation and execution; securing and hardening your images to reduce the attack surface; patch software; establish baselines so you can identify good from bad; controll administrative accounts and strengthen passwords; better yet, add in two-factor authentication. All of these can significantly stop or restrict an attacker.

Theresa Azari: In an era when more employees are working remotely from home, we need to be mindful about extending good security practices beyond the traditional corporate infrastructure. This would include solid security protocols for employees who may be using their personal devices for work (BYOD); ensuring that remote access and correspondences are secure (encryption – VPN) and authenticated before access is authorized (multi-factor authentication, strong passwords); activat strong login credentials by default (remember Zoom bombing?); and be extra vigilant of threat actors to reach out remotely (exercise caution when opening attachments, validating the identity of the source before providing data). Now, more than ever, there needs to be transparent and executive level oversight (CISO or equivalent) to ensure successful implementation.

ThinkTWENTY20: *Are the new security policies driven by the COVID-19 work-at-home situation likely to impinge on personal privacy of employees?*

Nair: Privacy should never be a barrier to drive business or security objectives. Instead, it should serve to bolster them, but that requires building privacy into the design of your people, process and technology upfront.

There are a host of privacy concerns that come up with the new world of work-at-home driven by COVID-19 and an eventual return-to-work. These emerging privacy issues include:

- Proactively monitoring employees working at home to ensure compliance with security policies and to assess productivity.
- Screening employee health status prior to an employee returning to the workplace to

maintain a safe work environment.

- Tracing employee information to identify if you have come into contact with an infected person and to minimize the spread (“contact tracing”).

Despite a patchwork of privacy rules around the world, what is consistent is that they are based on core privacy principles and should not inhibit the ability to process data in the fight against COVID-19. Ensure, for example, that you use personal information only for legitimate, reasonable and proportionate purposes, with clear legal authority and transparency on why you are collecting this information, such as through an employee notice or privacy policy.

If anything, the current pandemic has highlighted the importance of employee privacy, which in some countries such as Canada has arguably taken a back-seat for many years to customer personal information protection.

> Even when organizations spend thousands of dollars on the latest and greatest technology to protect their assets, they are only as secure as their weakest link, their people.

Gupta: As a result of the COVID-19 pandemic, most employees were required to work from (WFH), and supervisors/managers could not physically see their employees and understand what work was being performed or to what extent. Questions started to arise around productivity within vs. outside of the office. This, along with other WFH security concerns, such as insecure laptop configurations or home networks, has increased the prevalence of remote tracking software. The tools presently available have the ability to mirror employee activities, take periodic screen captures and log key strokes, meaning anything they do can potentially be tracked and recorded. The logging and monitoring of all employee activities can result in privacy and legal ramifications as well as it can affect company culture by creating distrust among its personnel. With insider threats being a significant risk to any organization, strong consideration should be given prior to implementing any such tracking and monitoring software.

Brown: The response to COVID and security has been varied across sectors and individual organizations. Generally, we have seen larger, mature organizations effectively transition to remote work with very little disruption. They have implemented well defined policies and combined these with mature technical controls. This is essentially an extension of the normal work environment and there are few, if any, impacts on personal privacy.

The bottom line is that governance and technical controls are important and need to be planned in advance if this issue is to be managed in a way that respects both the requirements of employers and the rights of employees.

Theresa Azari: Not necessarily, as employees will not be divulging personal information that the company does not already possess. In actuality, these new security practices may even help enhance personal privacy by addressing/fixing vulnerabilities that the employee is not even aware of (e.g., malware on their personal devices).

ThinkTWENTY20: *Do you see the main threats and solutions changing over the next few years? Will security be forever changed in a post-pandemic world?*

Nair: Economic downturn combined with new ways of working will introduce new risks and opportunities for all organizations in a post-pandemic world. Some key trends and considerations include:

- During an economic downturn there are increased insider threats-related risk due to employees being more likely to be disgruntled, bribed or coerced.
- Employee medical information will need to be handled in a privacy-compliant way to enable return to work efforts.
- Organizations will need to modernize their cybersecurity functions through digitization, analytics and automation to be more cost effective and manage headcounts.

- The push for more services for customers via online or mobile will require organizations to approach security, privacy and fraud risks in an integrated way, through all digital channels to improve customer experience.
- Efforts to improve technology resilience through cloud adoption and deperimeterization of enterprise networks will require uplift to security architecture and solutions.
- Reconfiguration of supply chain using automation and digitization (e.g., IoT, OT, 5G) will need to consider sufficient security controls to minimize safety and reliability risks.

Gupta: The fundamental concept of information security will not change in the post pandemic world but, as more and more organizations transform digitally and take advantage of the latest technologies such as Internet of Things, cloud computing and artificial intelligence, the threats will become increasingly more complex to navigate. In conjunction to this, cyber criminals are becoming more sophisticated in their usage of various tools and techniques.

On a positive note, security solutions (Identity and Access Management, Cloud Based Data Recovery, Security as a Service, End Point Protection, Vulnerability Scanning, etc.) are becoming more advanced and automated, and cyber security is now a priority for most organizations.

Brown: The threat spectrum is constantly evolving, as the cyber criminals adapt their techniques to circumvent improvements in security and seek to maximize their profits. Methods can be expected to change as a result of advancing technology and the infusing of artificial intelligence and machine learning into both attack and defense solutions. The continued move toward cloud computing and the Internet of Things will only increase the attack surface.

Theresa Azari**:** In a post-pandemic world under the new normal, one of the biggest challenges will be how to balance a person's privacy with new security protocols to support physical distancing and contact tracking mandates. We can expect that hacking activities will continue to heighten exponentially, making it more challenging for organizations to keep up with the change and higher risk levels. Before COVID-19, cybersecurity programs were based on regulatory frameworks such as NIST, ISO 27001, PCI DSS, or GDPR. These frameworks will need to evolve also in the wake of privacy considerations.

ThinkTWENTY20: *With all the solutions out there, why is cybercrime still increasing exponentially?*

Nair**:** Cyber risks are complex and dynamic. In our 23rd PwC CEO survey, 90% of Canadian CEOs say the increasing complexity of threats is having the greatest impact in shaping their cybersecurity strategy. There are three important factors complicating cyber risk management:

- Drivers external to the organization, such as new threat actors and attack methods, new technologies, geopolitical tensions and socioeconomic pressures are continuously changing the cyber risk profile.

- As organizations pivot toward a digital business model, exponentially more data is being generated and shared among organizations, partners and customers, exposing them to new vulnerabilities.
- Organizations are struggling to meet the increasing expectations of their regulators relating to cybersecurity and privacy, especially Canadian organizations operating in multiple jurisdictions around the world.

Gupta: Cybercriminals are harnessing the power and interconnectivity of the internet to successfully execute attacks from anywhere in the world. Cybercriminals can launch large scale attacks with very little investment. It's fairly inexpensive to launch an attack. Most people today have some sort of online presence via social media that may contain details about their occupation, place of employment, home address, email address, etc. The combination of businesses moving more activities online, combined with personal information being readily available, has made it a breeding ground for cyber criminals to execute targeted attacks on employees, superseding technical protections. In addition, scams are continuously evolving. COVID-19 phishing emails or malicious case tracker websites are a recent example of this. As long as cybercrime remains lucrative, it will continue to increase. It is up to all of us to remain resilient in our fight against cybercrime.

Theresa Azari: Even with all the technology solutions out there, it's not the magic bullet. Several factors to consider: 1) organizations fail to understand where their security priorities should be, making it hard to clearly understand where funding should be spent; 2) not having the right security team on board to assess, deploy and manage the right solution for their unique environment; 3) insufficient budget – it's a challenge to get budgetary approval to purchase these security tools when there are conflicting initiatives which also require funding.

> By applying controls against endpoints, users, data access, etc., the kill chain of many common attacks can be broken and the client protected.

Brown: Cybercrime will continue to increase because the valuable data, capable of being monetized by criminals, is largely contained in a cyber environment. This is only exacerbated by the rush to adopt cloud computing, distributed data stores, smart devices and remote workforce practices.

There are several disturbing trends that contribute to cybercrime. The increasing sophistication of rogue state actors and organized crime groups presents a level of capability requiring continual diligence on the part of a defender. There is also a trend toward softer targets, such as individuals or small and medium companies that do not have large budgets for cyber security, because there is still a lot of money to be made from these victim groups.

Elevating the threat to these targets is the commodification of cybercrime tools and technology, such as “hacking as a service,” where a customized malware or virus can be purchased for as little as $50 on the dark web.

This question also identifies one other problem: many “solutions.” This reinforces the point that many organizations look at security as something you buy and not something you do. They purchase a solution, which can be effective in reducing risk; but, to be completely effective, a solution needs to be considered within the context of the risk envelope and operate as part of a layered program of governance, risk management and compliance.

Why is cybercrime increasing? Willie Sutton, when asked why he robbed banks, was quoted as saying “Because that’s where the money is.” This is equally true for our cyber environments.