ISSA DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Third-Party Risk and Threat Hunting

By Gregory Rasner – ISSA member, Raleigh Chapter

This article describes cyber third-party risk steps and best practices and expands into a new mind-set: third-party threat hunting. This new approach to how firms manage their cyber risk with vendors moves from a compliance, check-box type activity to an ongoing and engaging method to improve the security and stability of both vendor and company.

Abstract

This article describes cyber third-party risk steps and best practices and expands into a new mind-set: third-party threat hunting. This new approach to how firms manage their cyber risk with vendors moves from a compliance, check-box type activity to an ongoing and engaging method to improve the security and stability of both vendor and company. Starting with point-in-time assessments and how to improve upon these needed tasks, the article discusses continuous monitoring, legal language, cyber expertise, and emerging areas: fourth-party risk, zero-trust principles, and the use of analytics. Cyber activity has significantly increased since the pandemic, and it has exposed this cyber risk area as under-performing for many companies. This article offers options for both small shops to multi-national companies.

The threat landscape has changed as cyber attacks are on the rise. Third-party risk for the last several years has evolved and many companies are tackling this risk by forming policy, processes, and people to perform the duties. It has largely been made up of intake security (along with other domain assessments), a periodic remote assessment (where a question is sent to a third party), and even fewer onsite assessments (going to the physical location of the vendor to have them physically validate security controls). In addition, many firms are adding information security terms and conditions, either directly in master service agreements (MSA) or as a separate attached exhibit. However, these activities were largely adopted only by firms that were regulated to perform these activities, large public firms that had board risk committees demanding action, or a few more forward thinking companies.

The policies, processes, and people have performed this largely as a “check the box, next action” compliance activity. The pandemic and resulting heavy increase in cyber activity, combined with the inability to perform onsite assessments, showed a weakness in approach for those currently doing third-party risk. Companies can no longer ignore vendor risk whether in a highly regulated field or not; it doesn’t matter because between privacy laws and the potential losses due to direct costs and reputational hit, *every firm* will be regulated in some way and financially obligated to determine how to ascertain risk appetite with vendors and manage it more proactively.

Countless firms and companies have been hit with ransomware, phishing attacks, social engineering, and advanced persistent threats [11]. This means your vendors are also increasingly getting attacked. Every firm is someone else’s third or fourth party. Third-party risk must now evolve into a more active and persistent action. This is best accomplished by evolving best practices around five key areas:

1. Engaging vendors in security conversations, not checklists
2. Publishing legal language that addresses your company’s cybersecurity risk
3. Designing a team that can perform continuous monitoring of your third parties
4. Hiring cybersecurity expertise and experience
5. Performing third-party threat hunting

Vendor due diligence and engagement

A third of companies have only an ad-hoc or no significant third-party risk process [7]. Over fifty-percent of companies admit to not monitoring the security of their vendors [6]. The cyber third-party risk team must have three key areas covered to identify and quantify risk to the organization.

First is the security evaluation intake process, where the team has a set of questions for the third party to answer via a questionnaire, which allows evaluation of what the vendor attests to about its security controls and program. This process informs the business of key risks that the vendor is recommended to close before production or at some subsequent date that is acceptable to internal risk appetite.

The second activity is onsite assessment, where the firm will send its own team of cybersecurity experts to the third party's site to physically validate that security controls are in place. This onsite assessment is generally more in-depth and allows for sharing of more confidential information than a third party would likely be comfortable sharing remotely.

Lastly is a continuous monitoring program that performs ongoing due diligence of vendors that meet risk criteria.

The first two assessment types are valuable to provide security information on the vendor, but most companies employ checklists, nothing more than a series of questions with options, yes/no drop-downs, and explanations of compensating controls but misses the key advantage of being physically at their location. A vendor is a partner helping your company to be more efficient or make more revenue. Engage in conversation with them about their security program, design, and implementation in production. Having an eye-contact discussion builds relationship and develops trust, for example a checklist on access management versus a conversation about the same. The checklist would provide information such as password complexity rules, history, and aging. A conversation would start with asking to view the company's access management policy, looking at when was it last reviewed and approved. This can lead to discussions about how the policy is enforced and when last reviewed, during which time the security assessor can be looking for any apprehension or body language that would be a "tell," in the poker parlance. Most people want to be honest and transparent and when something makes them think of a potential weak point in their security, this comes out in a conversation. Remember, this is a partner who is important to your business so unless any risks found outweigh income or efficiency, then any risks identified are shared with them, collaborating on an agreement for remediating the risk.

Conversation is more important now in the current climate of no travel and social distancing: onsite assessments are not taking place and likely will not in any large way until a vaccine is available. Leveraging any number of online collaboration tools that support video conferencing can fill this gap—being able to negotiate how to perform this activity over a web conferencing tool can be challenging. Eventually onsite assess-

ISSA JOURNAL
OFFENSIVE CYBER OPERATIONS ABROAD
INFLUENCE US CONGRESSIONAL LEGISLATION
ISSA JOURNAL
The Ethical Use of Machine Learning in Cybersecurity
ISSA JOURNAL
Secure DevOps before DevSecOps

ments will begin again, but until then companies should not stop this activity but leverage the work-from-home tools we're already using. Identify your systemically critical vendors and begin discussions about video conferencing "virtual" onsite evaluations. If the vendor has a data center, leverage any artifacts that are available—SOC2 Type II reports, independent audits, etc.—until a physical appraisal can be done. If the vendor has your firm's data at a cloud service provider (AWS, Azure, Google, Rackspace), then request a configuration report for your tenant: AWS Trusted Advisor Report or Azure Security Center.

A vendor is a partner helping your company to be more efficient or make more revenue.

If you are in a firm too small to perform these types of onsite evaluations (virtual or physical), there are consortiums that allow you to purchase them (remote and onsite). Keep in mind, these consortium-based reports are not risk assessments, but data feeds; most industry regulators require the company to perform the risk assessment of the data provided by the consortium. You cannot outsource your risk-assessments or risk appetite.

The frequency of onsite and remote assessments is based upon risk. Depending upon your organization's size and risk appetite, your firm may choose to do hundreds of assessments a year or focus on a few strategically critical vendors. This decision should flow from an executive leadership discussion about risk appetite, risk exposure, and obligations to shareholders or customers. Much of this is also driven by legal requirements about privacy.

Currently, only 19 percent of organizations report conducting security assessments on their third-party data handling practices [6]. There are too many *not* performing these activities.

Information security legal language

Only 44 percent of companies hold their third parties to contractual terms for cybersecurity [6]. This lack of contractual security language leaves both parties unprotected in the event of a breach or event. A company can address this risk by adding language in their master service agreement (MSA), or

Women Making It Count

Continued from page 6

- Follow social media influencers, especially women in STEM.
- Get girls to pursue STEM early through classes and career exposure in middle and high school.
- Provide externship opportunities to students so that they can see workplaces/spaces in STEM careers.
- See the impact of the Verizon Innovative Learning program for rural girls.
- Encourage applications for the NCWIT Aspirations in Computing Award.
- Share the National Alliance for Partnerships in Equity resources with girls in STEM/manufacturing.
- Participate and tune in to the new, international talk show, The Bridge for Women Worldwide.
- Participate in relevant employee resource groups for women, STEM, and diversity.
- Mentor college students entering STEM through clubs and chapters such as Women in 3D Printing association, Information Technology Senior Management Forum, the Society of Women Engineers, and Girls in Computer Science.
- Join the International Network of Women Engineers and Scientists.
- Host a conference like "Girls STEM Day" or "Futures Unlimited" for middle school to college students and gender expansive students.
- Fund a STEAM lab with a focus on girls and underrepresented communities

Conclusion

When we come together we are more effective. Women can help organizations understand the importance of diversity and inclusion in the workplace. Women can help other women seek and find their area of passion to plug in and be counted. As women leaders in ISSA and other cybersecurity groups, we have a responsibility to let our voices be heard and to be our confident, authentic selves. In what areas are you passionate? Knowing the answer is where you can make yourself count. Just as there are many STEM fields, there are so many areas to actively pursue within cybersecurity. We need to encourage one another to plug in and contribute. Collectively, we make it count.

If we own it, we can change it.

References

1. Million Women Mentors, (2020), STEMconnector – https://www.millionwomenmentors.com/home-mwm.
2. Thinking Media, "Make It Count National Virtual Event," Learning Blade, August 2020 – https://www.youtube.com/watch?v=g2OG5Z-jd7Ns&feature=youtu.be.

About the Author

Dr. Curtis C Campbell is VP of Atlantic Capital Bank in Atlanta, GA, a recently elected ISSA international director, and also serves as ISSA Chattanooga Chapter president. Curtis holds a PhD in Organizational Leadership in Information Systems Technology and serves on the advisory board of University of TN-Chattanooga, a national Center for Academic Excellence for Cyber-Defense (CAE-CD) studies. Connect with Curtis via curtis@mprotechnologies.com.

if the risk is sufficient, having a separate document for information security risk. Whichever approach is taken, security controls and enforceability need to be balanced. It might be tempting to include a long list of security controls required, but this can lead to long and expensive delays in contract negotiations. Focus on key security risks, based upon your business. If your protected data is going to be managed by the vendor, then ensure to focus on high-value items such as encryption and access management; if they'll be connecting to your network, ensure items such as encryption, access management, and patch management (if the vendor's equipment is used for connectivity) are in your documentation.

The legal documentation is a collaboration with your legal team (whether that's internal counsel or someone retained externally) and cybersecurity leadership. The document is owned by the legal team as they are the experts on the specific language to protect the firm; the cyber team owns the security terms in the document and works with legal to have those risks addressed with the proper legal language. As part of the sourcing process at a company using this type of exhibit or language in an MSA, when the vendor meets certain conditions (vendor is going to have access to protected data or a connection to your network) then this cybersecurity language gets added [8]. If you do not have a legal department, there are examples that an Internet search will provide [3].

Once the firm has placed the language in the MSA or as a separate exhibit, there will be contract negotiations and there will be times where criteria in your language cannot be met by a vendor. Yet the business may still want or need to do business with them, so there is a risk review and acceptance process. It is important for the third-party risk team to risk rate this gap in the criteria, and it needs to be logged in a system of record. If there is a determination to accept the risk, then that data is important to track for both continuous monitoring and third-party threat hunting.

Continuous monitoring

Of the companies that perform any third-party risk, nearly all interactions with vendors are point-in-time. It can range from at least 364 days until they are looked at again. That is a vast gap of time in terms of cybersecurity threats as they evolve, and it is an unhealthy trust of your partners' ability to keep up with them. 37 percent of companies believe their third party would not inform them of a breach [9]. There needs to be a mechanism or program to assess the security of your vendors in-between these point-in-time assessments.

The need to continually monitor third parties might beg the question: aren't vendors monitoring themselves, much as your own firm does? Yes and no. Companies, partnerships, LLCs, sole-proprietors are all run by the same: humans. Humans vary and so the attention to their own cybersecurity varies as widely. Being proactive has become essential as the cyber activity increases.

Continuous monitoring can take several forms, from using the multitude of vendor reputational scoring software available to having set intervals with key vendors to check-in on their performance. The key to success on the continuous monitoring program is to incorporate several data sources: vendor reputation software, cybersecurity intelligence, internal and external security assessments of the third parties, and

any other available sources to build actionable intelligence to approach a third party with a security concern.

Most vendor reputation tools use a combination of sinkhole technology (a passive way to observe behavior of the vendor enterprise) and cyber threat intelligence (and some other secret sauces that vary by software maker) to produce a score or value to present an easy visual of the risk. However, focus on the key indicators underneath: botnet infections, spam propagation, open ports, security incidents, and others. Set thresholds and alerts to get updates on your key vendors for these key risks. As these alerts come in, compare them with your own internal due diligence.

Let's try a hypothetical process to illustrate: An alert comes in for your key data analytics company, We-Do-Data-Analytics Inc (stores your protected data in a CSP), that states they've got some open ports (FTP) and botnet infections. Opening up a report from the onsite assessment performed on them by your firm last year, there is a finding that says they don't have any data loss prevention (DLP). In addition, there was an accepted risk by your company that the analytics company couldn't agree to limit administrative control on end-user laptops.

Meanwhile the research on the botnet infections describes them as browser add-ons or extensions that have the potential to key-log and steal location information. Combining this information with the above data, it is now possible to engage with the vendor and discuss if the data your team have discovered can be confirmed with their internal cybersecurity team. It is possible that the information is a false-positive because most of these monitoring system tools are passive. By taking the key risk criteria alerts, combining with the internal due diligence data and your own research on the particular risk, this can help to tie all the data together, lowering the chance of a false-positive and providing something substantial for the vendor to investigate. If the discovery is confirmed as a security gap or incident, have the conversation and collaborate on a remediation plan.

A more active continuous monitoring avenue becoming available is leveraging the APIs and alerting coming from cloud service providers. At its simplest, most of them will provide alerts if any of their network or data centers are impacted by access issues. Setting up an alert to your team when (for example) US-EAST goes down for a CSP your vendors use gives you a head-start on any impact. However, it can be more specific and actionable. The major providers all allow API mechanisms to alert and perform actions based upon conditions [2]. For example, if someone turns off multi-factor authentication (MFA) for the root account on a cloud tenant, it can do anything from sending a text alert to automatically switch MFA back on. Going back to having an ongoing conversation on security with your vendors, it allows collaboration to find opportunities if they are using these CSPs. Leveraging these APIs to alert the team of a risk changes the dynamic and normal activity to continually managing vendor risk in near real time.

Cybersecurity experience and expertise

In most organizations, some of these third-party risk organizations are not inside the cybersecurity groups, but rather are in risk or vendor management areas. This results in a team that is risk-focused, but not necessarily information security risk-focused. While one of cybersecurity's main goals is to identify risk, risk does not necessarily always identify cybersecurity risk. As is shown time and again, it is cybersecurity risks that pose the largest financial and reputational risks to most firms [10]. Infosec organizations rely on professionals with distinct certifications and experience focused on cybersecurity that enable them to identify security gaps that represent risks.

In addition, experience and certifications specifically in cloud and/or network technology, ensure that the team can address the risks associated with cloud deployment, as these solutions become more attractive and valuable to companies across nearly every industry. Cloud solutions are, by their nature, nimbler and quicker to deploy, so having a team that is familiar and well-versed in these requirements allows them to identify and remediate risks with cloud more quickly.

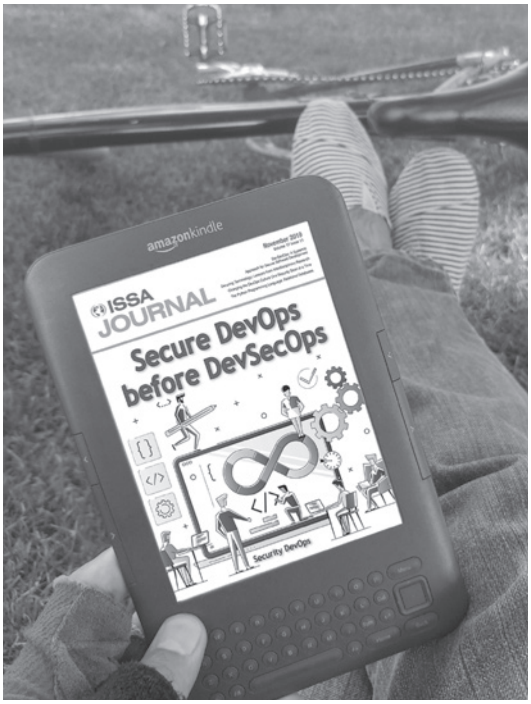
This team will be cybersecurity professionals and as such trained to identify risks in all three areas of the triad: confidentiality, integrity and availability. This can be viewed as an expansive scope to some organizations. However, that large scope is because, apart from the landscape company and golf association fees, nearly everything else goes over a wire as data. Cybersecurity professionals are trained to find the risks to how, where, and what is done with information. The team will form relationships with the vendors and form a partnership to increase both teams' security and stability.

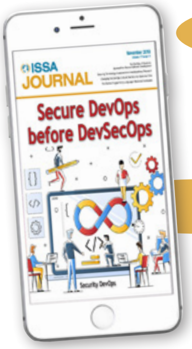
In smaller organizations, from a few hundred people or even sole proprietorship, the approach will be one of scale and risk. If you are a sole-owner or a few-people firm, spend some time looking at where your data (personal, financial, customer) is stored and any connectivity where that data is stored. If its online with one of the major providers (Google, AWS, Microsoft, etc.) and you are hands-on, there are plenty of FAQs and walk-thrus on their websites. There are also small local firms who specialize in this work; however, be sure you nail down your scope to avoid getting surprised at results and billing. For a mid-size firm with an equally mid-sized cybersecurity group, the choices for them become more broad: small boutique firms to large security advisory firms are easy to find and get a conversation going about scope and risk appetite. Consortiums exist that provide the remote and onsite assessments data to your firm, but then you must perform your own risk assessment of that data. From large technology firms down to the local security consultant, there are plenty of options, and as a firm grows it can transition that work internally if risk and budget dictate and align.

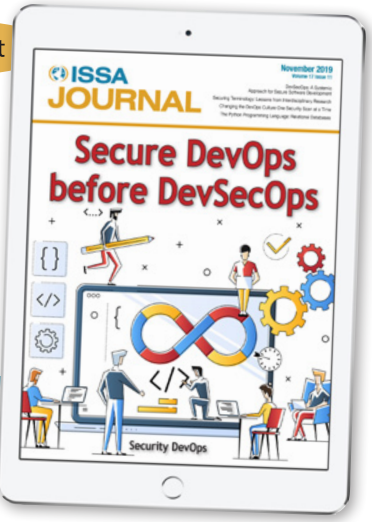
Third-party threat hunting

Third-party threat hunting is a mind-set change in the approach to this risk domain. First, while too many firms do not perform this due diligence, those that do, do so as a checkbox activity. The best evidence of this comes from infosec organizations themselves: when it is in cyber organizations, due diligence is most often placed in GRC teams (governance, risk, and compliance). It is a risk activity completed out of obligation, not out of need to survive as a business. The new approach is more at home in cyber operations (threat hunting, vulnerability and incident management) teams where there is an always alert staff actively searching for threats, risks, and vulnerabilities. On the subject of size and scale, if the company is small, then being engaged with vendors who have your data on how it is secured is a good start. Companies with boards and shareholders need to be asking direct questions about their organization's approach to third-party risk: is it the whack-a-mole approach with one mallet or do you get ten mallets and five resources to help you smash them all the time [7].

The next step in this threat hunting approach is to be engaging vendors for other opportunities to lower risk to both teams, for instance, vulnerability management for critical vendors. This approach can vary from keeping a list of hardware and software versions for your data is stored and processed. If a vulnerability is announced for one of them, engage the vendor to determine their plan for remediation or compensating







controls they're taking. For some very critical and high-risk business there could be discussions of consuming log files from the third party for internal review. Vendors are partners is your success and theirs; the limits of what can be done in collaboration or worked into a contract are only bound by your staffing and risk appetite.

Fourth parties are also on the list of the third-party threat hunting. Fourth parties are those companies that are third parties to your vendor. These are also risks that many do not even consider, let alone monitor [8]. If the fourth party processes, accesses, or transports your data, you are at risk. Currently the number of companies that collect fourth-party data is a minor subset of those who manage their vendors. Firms that do collect this data generally ask for it at intake and onboarding of the vendor. A very diligent firm will ask annually for an update. Because of the relationship, no due diligence can be done directly on a fourth party. One option to reduce risk, the remote and onsite assessment should inquire about the supplier's own vendor risk management process. However, monitoring them in a vulnerability management type process takes the proactive approach: alerting for an incident or security issue at a critical fourth party could mean quicker response to the threat.

Zero-trust principles are coming to third-party risk management. Connectivity to your network is potentially the biggest threat if not managed. Creating enclaves or DMZs where vendors can connect to your corporate network in a secure and quick manner is critical. Based upon the type of work the vendor performs, the risk it poses, the business need, and other factors will drive what these enclaves have access to. Examples would be a vendor connecting to work on customer records would require MFA, and monitoring of that connectivity would be higher than the supplier that connects to process your office supplies. Both would have layered defenses, but this segmentation allows more control and faster deployment. Another example: move any direct connections out of your connectivity closet and onto an edge provider, pushing the risk outward.

Analytics and reporting are typically point-in-time snapshots of what happened last month or quarter. There is very little reporting internally provided on the cyber risk for a company's third-party portfolio. However, the data is expansive in most medium-to-larger organizations. As your infosec trained and experienced teams begin to have conversations with vendors about their security, drafting better security language in contracts, actively seeking security gaps in continuous monitoring, all this data is collecting in the background:

- Security findings from remote and onsite evaluations
- Risks accepted as part of contract language
- Gaps identified in the continuous monitoring team

Other internal data sources likely also exist:

- Risk management tools
- Supplier risk software
- Cloud access security broker (CASB)
- Data intelligence feeds and others

Collecting this data and using it to make more predictive decisions is the next step. Whether using a simple business intelligence tool or an analytics engine, there exists the ability to take this data and get a cyber risk scoring for your vendors. The algorithm that determines what that scoring looks like will vary based upon your data feeds. Onsite assessments, where there's been physical validation of controls present, would weigh more heavily, while data from other sources (such as vendor reputation tool or a vendor's self-assessment like a SIG[1]) and similar would have lower values due to their lower level of reliability. In the simplest form, this can

[1] SIG (standardized information gathering questionnaire), Shared Assessments – https://sharedassessments.org/sig/.

be a graphical representation of each vendor's score in red, yellow, or green, based on thresholds and how vendors are risk-tiered.[2] This allows your team to focus on those in your highest risk, based upon this data being more proactive than waiting for notification of a breach. As the threat landscape changed in early 2020, third-party threat hunting takes an aggressive approach to lowering this critical risk now and in the future.

Conclusion

The focus on third-party risk increased over ten years ago with some early data leaks at large firms resulting from a vendor. Larger firms began increasing focus and those in highly regulated fields were forced to or face fines and oversight. Since the pandemic the ability to perform onsite assessment ceased while cyber threats increased [5]. The warnings had been there before the virus caused this to hit a new level [1]. Point-in-time assessments were exposed as insufficient in some cases due to the rapid increase and change of environment, changing the mind-set to an active, always-in-motion activity. Monitoring vendors, engaging with them to lower risks, holding them legally accountable in contract language, and continually monitoring for potential risks will lead to a more secure and stable business for you and your third parties.

References

1. ALM Media, "Third Party Breaches Are a Threat – And Many Companies Aren't Ready," Yahoo Finance, 21 November 2018 – https://finance.yahoo.com/news/third-party-breaches-threat-many-060036149.html.
2. AWS, "Amazon API Gateway, Developer Guide, Monitoring REST APIs," AWS – https://docs.aws.amazon.com/apigateway/latest/developerguide/rest-api-monitor.html.
3. Drye, Kelley et al., "Data Security Contract Clauses for Service Provider Arrangements (Pro-Customer)," International Association of Privacy Professionals (IAPP) – https://iapp.org/resources/article/data-security-contract-clauses-for-service-provider-arrangements-pro-customer/.
4. Jaeger, Jacklyn, "Reducing Fourth-Party Risk with Eyes Wide Open," Compliance Week, 8 May 2018 – https://www.complianceweek.com/surveys-and-benchmarking/reducing-fourth-party-risk-with-eyes-wide-open/2281.article.
5. Muncaster, Phil, "Cyber-Attacks up 37% over Past Month as #COVID19 Bites," Infosecurity Group, 1 April 2020 – https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month/.
6. Ponemon Institute, "Data Risk in the Third-Party Ecosystem, Third Annual Report," Ponemon Institute, November 2018, p3 – https://www.ponemon.org/local/upload/file/Data%20Risk%20in%20the%20Third%20Party%20Ecosystem_BuckleySandler%20LLP%20and%20Treliant%20Risk%20Advisors%20LLC%20Ponemon%20Research%202016%20-%20FINAL2.pdf.
7. Proviti, "2019, Vendor Risk Management Benchmark Study: Running Hard to Stay in Place," Proviti and Shared Asssessments – https://www.protiviti.com/sites/default/files/2019-vendor-risk-management-benchmark-study-sharedassessments-protiviti.pdf.
8. Sheehan, Amy Terry, "How to Maintain Effective and Secure Long-Term Vendor Relationships: Understanding the Risks," Cybersecurity Law Report, 20 June 2018 – https://www.cslawreport.com/2620296/how-to-maintain-effective-and-secure-longterm-vendor-relationships-understanding-the-risks-part-one-of-two.thtml.
9. Sher-jan, Mahmood, "Surprising Stats on Third-Party Vendor Risk and Breach Likelihood," IAPP, 21 August 2017 – https://iapp.org/news/a/surprising-stats-on-third-party-vendor-risk-and-breach-likelihood/.
10. Swinhoe, Dan, 'The 15 Biggest Data Breaches of the 21st century," CSOOnline, 17 April 2020 – https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.
11. WHO, "WHO Reports Fivefold Increase in Cyber Attacks, Urges Vigilance," World Health Organization – https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.

About the Author

Gregory Rasner leads corporate cybersecurity third-party risk at Truist Financial Corp. Prior, he held cybersecurity and information technology leadership roles in technology, biotech, and finance. Teaching part-time at local community colleges and volunteering time for veterans' causes are his passions. He may be reached at razman66@gmail.com.

[2] For example, a vendor with 1M protected data is a higher risk tier than one with only 2,000.