TREASURY&RISK
THE FUTURE OF FINANCE TODAY
An ALM Publication
JULY 20, 2017

Managing Risk in the Cloud: A Guide for Corporate Treasurers

What treasury managers need to know about cybersecurity, and how they can help guard their treasury management systems against threats.

BY ANDREW BATEMAN

Cyberattacks are incredibly widespread. According to the Kaspersky Security Bulletin, malware attacks were blocked on more than half (58 percent) of all corporate computers in 2015. Nearly one in every three business-owned computers (29 percent) was subjected to one or more Web-based attacks, and file antivirus detection was triggered on 41 percent of corporate computers. Headlines related to the latest high-profile hacks, security breaches, and data thefts are seemingly inescapable for anyone paying attention to the news.

Even corporate risk managers struggle to keep up with all the phishing, vishing, pharming, whaling, spoofing, baiting, spyware, malware, and ransomware terminology. Yet many treasurers are tasked with understanding and mitigating cyber risks. That's due in part to the fact that corporate treasurers' responsibilities have expanded significantly in recent years to include management of the company's complex risks, regulatory oversight, and treasury technology. Treasury teams are now far more strategic than operational, and are expected to add more value to the organization than ever before.

Treasurers also have ultimate responsibility for many of the areas most commonly targeted by cyber criminals, including cash balances, global bank connectivity, high-value payments processing, and maintenance of repetitive payment instructions. Corporate treasury and payments functions are frequently the targets of cyberattacks. And the recent SWIFT hacks, which hit home for many SWIFT for Corporates users, have contributed to a feeling within the treasury community that everyone is impacted by cybersecurity concerns.

Corporate treasurers need to be paying attention to cybersecurity. In other words, they need to be aware of where potential threats to their organization are originating, how they are evolving, and—maybe most important—what role they, as treasurers, should play in ensuring that operations are not disrupted by such an event.

"Cybersecurity" does not entail the management of one single, specific risk; rather, it is a general term that applies to any risk associated with information technology that has the potential to harm an organization. Like all modern IT risks, cyber risk has operational implications. For example, cyber risk managers must ensure that internal users' access privileges and segregation of duties are enforced at a systems level.

Risk managers and treasury staff should work together to ensure that users of the company's financial systems are trained in spotting and combating external fraud attempts that could compromise the security of corporate systems. These attacks might include bank impersonation fraud, IT department impersonation fraud, executive impostor fraud, phishing, and email attachment scams. In addition, treasury and risk management professionals should ensure that their static data is secure from external and internal threats and modification, by requiring secondary approvals and notification for all changes.

> "Many treasurers are suddenly finding themselves responsible for the evaluation of technology partners and strategies, and the cloud creates new risk factors."

Treasury's Responsibility in Cyber Risk Management

Treasurers historically deferred to either the IT organization or a corporate security function when it came to the management of technology-related risks. But many organizations have shifted away from this approach over the past several years, as cloud technologies have become more prevalent and treasury has become increasingly responsible for its own systems and data.

Cloud adoption rates have been skyrocketing in virtually every industry and geography. In a recent FIS market study, "Corporate Treasury—Rising to the Cloud," which surveyed over 100 treasury and finance professionals, 81 percent of respondents said they have migrated their treasury solutions to the cloud or think their organization is likely to do so in the future. The cloud has become the "new normal" in how treasury organizations consume technology. Many treasurers prefer cloud-based platforms for several reasons, including the facts that they require minimal internal resources for setup and maintenance, they may enable faster deployments and greater standardization, they can significantly lower total cost of ownership, and upgrades require minimal effort.

Like other executives, corporate treasurers are expected to own all the risks that impact their function. Many treasurers are suddenly finding themselves responsible for the evaluation of technology partners and strategies, and use of the cloud creates new risk factors that treasurers must consider as they select and establish relationships with treasury technology providers.

A treasurer considering implementing a software-as-a-service (SaaS) treasury management system should ask:

1. ***What type of cloud is offered: private, public, or both?*** Private clouds are typically dedicated, single-tenant application instances running on dedicated virtual servers. Public clouds, by contrast, are multi-tenant application instances running on virtual servers inside a shared virtual cluster connecting to shared database server hardware. The choice between these two deployment options will have implications for how the software is implemented, upgraded, and supported.

If a technology vendor offers both alternatives, make sure you understand the differences. Although public cloud solutions are often viewed as easier to implement and maintain, this is a viable option only if the corporate IT group is comfortable keeping treasury data in a shared application model of deployment.

2. ***How is customer data segregated in the cloud?*** You also need to understand and be comfortable with how your data is segregated from other customers in the cloud, because you need to be confident that your data will stay segregated. If you're interested in a public cloud solution, make your technology vendor prove the quality of its data segregation security and controls, so that you're sure your data will never commingle with that of other customers.

3. ***What security certifications does the technology provider possess? And how does it stay ahead of the curve when it comes to cybersecurity?*** Many cloud providers work with governmental agencies and third parties to continuously test the quality of their security. Certifications and security structure are absolutely crucial in ensuring customers' assets will be protected in the cloud.

4. ***Where is data hosted? And how secure are hosting centers?*** Data centers should use the highest possible levels of security, controls, and redundancy for both power and communication. Your vendor should also have a disaster recovery strategy that you and your IT group are comfortable with.

5. ***If you were to decide at a later date to bring your cloud-based treasury data in-house, how would that process work?*** This is an option you may want to learn about, so that you're prepared in case your provider suffers a serious hack or other security breach.

6. ***How is data encrypted?*** Encryption is the process of encoding data, messages, or information in order to ensure that only authorized parties can access it. The stronger the encryption capabilities, the safer your assets will be. Talk to your technology provider about its encryption solutions and about how it encrypts both data at rest and data in transit.

In another FIS market study, "Treasury Risk and Regulations: Tough Questions for Treasurers," a large proportion of survey respondents had not yet prioritized these risks sufficiently. The survey found that only 17 percent of corporate treasurers were treating cybersecurity as a significant priority for 2017, while 35 percent indicated that cybersecurity will have only a moderate impact on the development of their risk management strategies this year, and the remainder indicated that cybersecurity will have a minor impact on treasury and risk management strategies. Given the increasing types of cyber risks, and the potential financial and reputational implications of a failure, this is an area on which every

treasurer and risk manager should be focusing.

Responsibilities of the Treasury Technology Provider

Treasurers put faith in their technology providers and banking partners when it comes to secure solutions and best practices around mitigating IT-related threats. They should select treasury technology partners that will ensure the safety of their data and treasury operation. And then, before the partnership agreement is signed, treasurers should ask a technology provider to demonstrate its expertise and commitment to the security of the chosen solution, as well as explaining the role the vendor will play in advising and protecting the client. Treasurers should also remember that banking partners are in many cases treasury technology providers as well, and so should be put under the same scrutiny as specialized treasury technology vendors.

As part of their due diligence, treasurers should make sure that their selected treasury technology provider has a robust process for gathering intelligence about threats at three levels, and for putting that intelligence to work for its clients.

"The right vendor should be able to help you understand the risks that exist in the cybersecurity space and the tools available for managing them."

First is strategic/executive intelligence. This information provides a high-level overview of threats in the landscape that treasurers need to be aware of. Best practice is for a treasury technology provider to be planning projects to enhance and manage risk activities for the next 6, 12, or 18 months and beyond. This would include being able to demonstrate its understanding of changing threat vectors, security technologies, and risk management best practices in areas such as encryption, data protection, compliance obligations, and social engineering.

Treasury technology vendors should also have a well-established process for collecting operational/business intelligence. This information provides a threat assessment regarding specific problems and products impacted, and provides options related to mitigation of these threats. At this level of business intelligence, the vendor should share information about its policy coverage and the high-level tools it uses to manage and mitigate or remediate risk. This includes the overall risk management process and tracking of risks and issues. When you evaluate a vendor's sharing of operational/business intelligence information, you are looking for thorough and active scanning and regular penetration tests of all elements of the service.

And, finally, software providers need to gather tactical/defense application intelligence. This information comprises network-based indicators of compromise, multifactor authentication, device fingerprinting, browser information, known mules and accounts, user behavior that is atypical or unusual, etc. As a customer (or prospective customer), you want to understand what the vendor offers in these areas and how that can integrate with your own layered defense.

Treasurers don't have the time or internal resources to gather threat intelligence data, so they need to be able to rely on their treasury technology providers to collect this information, use it to develop risk-mitigating solutions, and advise their treasury clients on the threat environment. The right vendor should be able to help you understand the risks that exist in the cybersecurity space and the tools and options available for managing them. It should also explain the general best practices that all groups (treasury vendors and corporate treasury organizations alike) should be demonstrating.

Building a Cyber-Savvy Treasury Function

In order to mitigate cybersecurity risks to their systems and data, corporate treasurers need to focus attention on three best practices in the second half of 2017:

- ***Awareness/education.*** Create a cyber-risk–conscious treasury culture. Engage with your security team to stay current on threats and trends. Have the information security and IT groups regularly communicate simple best practices to the treasury team—for example, avoid reckless browsing, especially on public Wi-Fi hotspots; password sharing; irresponsible social media usage; etc.

- ***Investment.*** Invest in the right technology, systems, and tools. Stay on current releases of treasury solutions. Stay up-to-date on Microsoft security updates. Ensure that your antivirus solution is up-to-date with virus definitions. Strengthen technology used for preventative monitoring and detection controls, and have an incident response/action plan.

- ***Partnership.*** Leverage both your technology provider and banking relationships to understand the current threat environment. Partner with treasury technology providers selectively, choosing only those with demonstrated strength in managing these risks. The IT group should work closely with the treasury department in advising on best practices and helping to ensure that treasury can

The Near Future of Cyber Risk Management

In the second half of this year, we expect cyber risk management to continue to evolve as treasurers and organizations strengthen defenses. Here are six trends to keep an eye on:

1 **The greater interest from regulators related to threat intelligence and threat intel sharing.** Regulators and auditors are looking to every level of an organization to be engaged in the risk management of cybersecurity risk. This is now an area that the treasurer can expect to be asked about in regulatory reviews and by their board. Regulators want to see demonstrations that the treasurer is engaged in cybersecurity activities, and that the culture of security management has become part of every person's role.

2 **The continuation of merging of cyber network and cyber fraud indicators of compromise.** Cyberattacks are becoming increasingly sophisticated and targeted; they combine elements of vulnerability across many areas to create opportunity. Just as attacks are gaining in complexity and breadth, our security responses have to gain in depth and variety and be multilayered.

3 **The increase in mobile-device threats and attempts at exploitation.** Mobile devices are playing an increasingly important role within the portfolio of tools being used in the treasury space; mobile is also an easily and regularly targeted threat vector. This will continue to grow, and having an adequate mobile policy is critical, as it's not just the same as everything else we do.

4 **The greater sophistication of the criminal infrastructure.** Cybercrime has become commercialized, with many elements of it being commoditized. It's effectively a business in its own right, and we need to acknowledge that in responding to that risk.

5 **The availability of more vendor and sales information.** Organizations looking to undertake their own cyber risk management are faced with a multitude of point solutions in the cyber industry space that collectively are daunting—and the market is growing. Leveraging the scale of a technology vendor that is able to wrap this into their treasury solution package can be an effective way to help manage that complexity.

6 **The maturation and evolution of the threat intel space.** Threat intelligence, near–real-time sharing of threat data, and threat knowledge collaboration are growing trends amongst corporate and government agencies where previously this information was jealously guarded. Engage with this trend, either independently or through your vendors, to prepare to manage the risks to your business.

Source: FIS.

perform "daily blocking and tackling" effectively.

The scope and responsibility of the treasurer continues to evolve, sometimes in unexpected ways. The next generation of treasurers will look for more innovative, easier to use, and easier to consume technology within the cloud. But with the cloud comes greater complexity related to security and new kinds of risk. Treasurers have an increasingly important role to play in making sure they're doing everything they can to keep company assets safe.

Andrew Bateman *is head of treasury, payments, and receivables solutions for FIS. These businesses provide solutions to corporations for managing their treasury, payments, and messaging operations, and to banks for managing their own treasury operations and providing solutions to manage their customers' operations as well.*