THE EUROPEAN ASSOCIATION OF CORPORATE TREASURERS

Is your company protected from cyber threats?

Today's treasury infrastructure is changing and, with it, the associated risks of data loss or fraud have multiplied. Within the security community, it is often said that it is not a matter of 'if' but 'when' you are going to be affected by a security breach. Treasurers need to ensure that controls are in place to protect the corporate assets and, as such, should take a lead role in protecting the company from cyber threats. Securing your company is not a onetime exercise; it is a journey that needs to be reviewed regularly and adapted to new threats. The following is a collation of best practices gathered to help you on the journey to protecting your company from cyber threats.

You can't do it alone

It is unlikely that treasurers have the expertise to protect the company on their own. Therefore, it is best to create a cross-business team with technology, information security and internal audit to jointly protect the firm. Working together and utilising collective expertise, the team can audit risky processes, run security penetration tests, and then jointly assess the levels of risk to the organisation before determining an action plan.

In addition, this is not something that only the leadership team needs to be aware of. To best prepare the organisation, the employees need to be aware of the latest fraud schemes and techniques, and receive proper training on how to successfully identify, prevent and respond to attacks. This training must be provided regularly, so as to keep pace with the constant evolution of the cybercrime landscape. It is a good idea to test the effectiveness of the training through mock phishing exercises internally to ensure the employees follow the proper policies and procedures.

Protecting the treasury infrastructure

There can be numerous entry points into a company's infrastructure. For some, all it takes is an employee plugging in a USB stick they found on their way to work, or an unintentional click on a website (even legitimate ones) to open the infrastructure up to risk. It's a good idea to review these potential entry points with your technology team to understand what controls you have in place. The below topics provide a good starting point for these discussions:

- How is your treasury infrastructure (servers, switches, storage, routers, modems, leased lines, etc.) physically restricted from tampering?
- Do machines with access to the treasury infrastructure have unused ports and external access ports (e.g. USB) blocked to prevent someone installing malware? Do

any machines on the network have access to the internet or email where someone could accidently download a virus/malware? If so what mitigations are in place to reduce the risk?
- Do all the systems in the network use a firewall, antivirus, have up-to-date operating systems and antivirus signatures?
- What level of authentication is used for key users (e.g. admin or payment authorisers)? Is a username and password sufficient or should two-factor authentication be considered?

Minimising the risk from external connections

You need to protect the information not only whilst it is within your environment but also when it leaves your estate. To do this, the key is to instigate encrypted channels and protocols throughout the information flow. There are a number of weak points to consider:
- Does your system extract the data from the ERP system and then encrypt it or does the data come out encrypted? If it is extracted unencrypted, who has access to the folders where the data is stored?
- If you have any systems on the cloud, is your cloud provider ISO 27001 certified? Does your cloud provider transfer data to unsecured servers at any point? Are employees from the cloud provider vetted?
- If you are using a SWIFT service bureau, do they have certification from SWIFT to operate and can they provide a SAS70 type II audit report? Are they compliant with the latest version of SWIFT SIP Release to attest their level of security?
- If third party vendors have access to your network, are their cybersecurity controls and incident response appropriate for the services they provide and access they have?

When considering regular penetration tests, you should think not only about your treasury infrastructure but also that of supporting systems and your external service providers.

Manual interactions

Manual interactions within most systems are inevitable. When they do arise, the key is to ensure there are the appropriate levels of control around them. Utilising features such as user profiles, workflow limits and four eye approvals help. However, for controls to be effective, you also need to ensure users have just enough latitude to complete their jobs. When determining where controls are required within the workflow you should think creatively. For example, whilst the payment details obviously require a high degree of control, what about suppliers' phone details? If someone first modified a supplier's phone number and then changed the invoice details, would you call the correct number to check if the supplier's details are correct?

THE EUROPEAN ASSOCIATION OF CORPORATE TREASURERS

Utilising the controls available to you

Your banking partners may have a number of controls that can be deployed to further help you. The usefulness will depend on you integrate them. Below are the most common tools:

- Restricted payee lists, such as to only allow payments to credit pre-loaded beneficiaries / internal accounts.
- Workflow tools to aid dual approval and segregation of roles
- Two-factor authentication or one-time passwords for key users
- Reduced scope of individuals with dual administration.

Tracking unusual behaviour

Once you have implemented a tight control framework, you should consider how you monitor the payment flow, privileged user actions and network traffic to identify any unusual behaviour. The first step is to have a centralised role completing the monitoring. In doing so it helps build up expertise, in order to enable more effective vigilance and the creation of more useful controls. Advancements in technology, with respect to machine learning and artificial intelligence, are making this activity less resource-intensive and thereby accessible to more companies. When deployed to monitor network and server logs, you can detect threats before your antivirus is even aware of their existence. Additionally, when deployed to monitor users with privileged access, you can track unusual activity preventing account compromise and insider threats.

Incident response

Speed and precision are required to prevent an incident becoming a disaster. You should make sure the relevant actions are defined for each scenario, from the discovery until conclusion and review, as well as ensuring that everybody involved in each action knows their role within the process (compliance, audit, security, treasury, IT, banks, legal, corporate communications etc.). It is recommended that you regularly test the process to confirm the validity.

Conclusion

In some cases, the above practices may seem daunting to the uninitiated. Nonetheless, with the rising level of threats, it is paramount that attention is given to ensuring the firm's assets remain protected. A useful starting point would be to create a cross-business working group to consider your firm's potential vulnerabilities. Once you have a list, you can ensure management are aware and then prioritise the remediating actions.

THE EUROPEAN ASSOCIATION OF CORPORATE TREASURERS

About the authors:

This article was created through the collaboration of Anne-Catherine Sailley, and James Henderson as part of the European Association of Corporate Treasurers' CyberSecurity Working group, helping corporate treasurers to protect themselves from cybercrime.

Anne-Catherine Sailley

Anne-Catherine is working in Steelcase where she currently takes the Treasury lead in designing the banking structure to support more centralized payments, to drive the design of ongoing control structure around payment processes.

James Henderson

James is a Fellow of the UK's ACT and is Head of Specialist FX Product at Barclays Corporate Banking, supporting customers with integrated treasury solutions

.