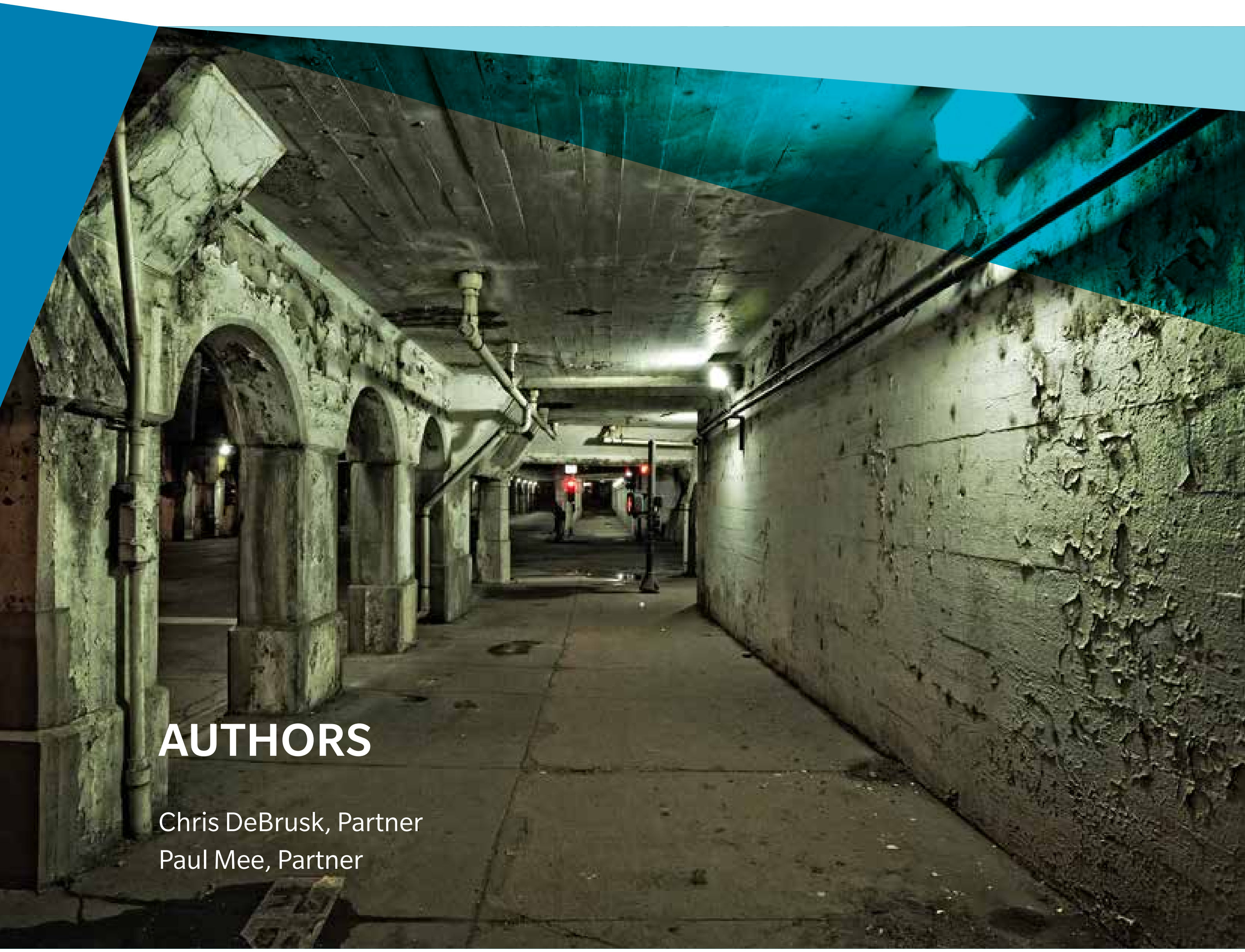
OLIVER WYMAN

CYBER RISKS THAT HIDE IN PLAIN SIGHT



AUTHORS

Chris DeBrusk, Partner
Paul Mee, Partner

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

Predictions for the aggerate global cost of cybercrime vary, but in every study or analyst report, the numbers are huge. Correspondingly, the amounts companies are spending in an attempt to protect themselves is also large, estimated at approaching $1 trillion annually in a global basis by 2022. Yet despite the clear recognition of the risk that cyber-crime and cyber-terrorism present to both individuals and companies, there are areas of hidden cyber risk that are either missed in audits or deprioritized due to the impact addressing them would have on a company's operations.

There are a whole range of data, process, and tools related cyber risks, that are often overlooked when audits are performed. In this article we explore ten of the more common "hidden" cyber risks prevalent in large and mid-sized organizations, and offer some suggestions on how to begin to address them.

END USER COMPUTING

Microsoft Excel is a favorite in most organizations. It is used both for its original intent, financial modeling, but also commonly for data capture, data management and enrichment, data visualization and to build proxy business applications using interlinked sheets and complex macros. Not surprisingly, one of the most requested features in business applications is the ability to download information to Excel or comma-separated value (CSV) formats or establish a connection between an Excel spreadsheet and a back-end database to support direct querying of information.

Putting aside the substantial risk of malware being inserted into Excel files, these end-user-computing (EUC) tools are potential pools of sensitive information that create an attractive target for cyber-attacks. Once sensitive or critical information is put into an unencrypted format it is essentially uncontrolled in most organizations. Even if it is encrypted, protections are generally easy to overcome using brute force attacks, given that few people use long passwords. These Excel and CSV-based data dumps end up on laptops, shared drives and SharePoint file repositories. They are also emailed around and will often sit in email inboxes and archives for extended periods, creating an attractive target for hackers.

Perhaps even worse are Microsoft Access databases, possibly one of the most problematic EUC platforms from a cyber risk perspective. Given their ability to ingest and store vast amounts of information and the relative difficulty in securing the platform plus the fact that the normal user is not typically an IT expert, Access databases can be a rich target for hackers.

BUSINESS INTELLIGENCE TOOLS

The proliferation of business intelligence and visualization tools like Tableau and Spotfire across organizations has resulted in significant business value. Users are able to see and interact with data in ways they could never achieve when a spreadsheet was the primary visualization tool on the desktop. Yet these tools have created a new area of cyber risk because they allow users to write queries directly against underlying databases.

The cyber-risk profile further rises when the designer of the visualization performs a wide-ranging query from the underlying database. Even though they may only be showing aggregated values on a dashboard, the details behind them are available for download, and may contain sensitive information that is not necessary for the visualization but inadvertently included in the query such as employee IDs on a query of monthly sales by employee.

Where databases are properly secured with role-based limitations, the risk that someone gets access to information they shouldn't is relatively low. But again, these tools create risk in that they allow the information that underlies the graphs and dashboards to be easily downloaded to CSV format. Once that step is taken, the data that was encrypted and controlled in a database is loose in the organization.

ROBOTIC PROCESS AUTOMATION

Robotic Process Automation (RPA) tools are all the rage these days. These tools allow "bots" to pretend to be human users and interact with applications directly to perform tasks. Many are desktop applications that allow non-technical users to write scripts to automate work, removing the need for IT staff to develop and implement automation capabilities. Even though these tools are a boon to cubicle bound workers in that they allow repetitive tasks to be automated, they are also a potential area of hidden cyber risk.

Envision a situation in which the user of an application that holds sensitive information needs to make a large number of record updates but doesn't want to do them one-by-one using the application's user interface. So, they quickly pull together a script in an RPA tool to access the application and copy a set of information on each customer to an Excel file. Then they use Excel to make all the necessary changes and write a second script to re-enter the changed values via the application's screens. From their perspective, they saved themselves and the company a lot of time, and quickly completed the task so they can get on to more important work.

Of course, the Excel file that was created and that very likely contained a range of sensitive information was stored in a convenient location, perhaps a shared department folder or even worse, their local laptop hard drive. It was also unlikely to have been deleted once the task was completed and is now a rich target for any hacker that managed to get into the company network but hadn't yet figured out how to access the cyber hardened application that the information was extracted from.

BUSINESS PROCESS MANAGEMENT

Business Process Management (BPM) tools have been deployed across organizations for over twenty years and can have profoundly positive impacts on productivity when leveraged to support complex workflows and move users out of email for business interactions – which can actually reduce cyber risk. Unfortunately, these tools, whether deployed independently or as part of a business application, can increase cyber risk as well.

As a complex workflow progresses along its steps, to facilitate a complex business process, users annotate the audit log of the workflow with information outlining what they did, issues they ran into and just general information for the audit trail. This is all good and expected.

The cyber risk issue is introduced when users copy sensitive information from cyber-hardened applications into the BPM tool's free text fields in an attempt to document their actions and facilitate decision making by others in the workflow. This information has therefore moved from a protected state to a state in which the protections have not followed. That creates a potentially rich target for hackers to take advantage of.

SECOND TIER SAAS APPLICATIONS

The use of business platforms that are provided as Software as a Service (SaaS) can often provide material benefits to a company. Examples of these platforms include Salesforce, Workday and others. While the third party cyber risks of any SaaS platform need to be established and understood before deployment, these processes are usually formally performed prior to the launch of the platform and periodically reviewed as cyber audits that are done on critical third-party vendors.

A potential area of cyber risk that isn't well managed is introduced by SaaS platforms that don't support core corporate functions. They include websites that manage surveys, handle charity events, facilitate employee and contractor fingerprinting, etc. Many organizations leverage these types of SaaS applications but rarely perform even a cursory audit of their cyber risk, assuming that the data that is shared with them is not sensitive. Yet, when you upload a list of all your employees, their departments and supervisors and their emails to a website to run a survey, you've potentially given a hacker a rich trove of information that can be used for phishing and other nefarious purposes.

SHADOW IT

Many IT organizations these days are overwhelmed. In addition to trying to service business needs for technology, they are dealing with a long list of challenges including cyber risk, business continuity planning, offshoring and outsourcing, legacy platform modernization and just generally hitting their cost reduction targets. So, it is not surprising that they cannot meet every business request that comes along. Perhaps also not surprising, there are many software vendors and professional services firms who are more than happy to lend a hand to deploy tools and talent to create new business capabilities when internal IT is stretched.

When this happens and central technology and cyber teams are not directly involved, shadow IT is created. These projects and the capabilities they implement are either not, or only partially within the control of IT and as such often don't follow the rigorous standards that are being defined and implemented across organizations to reduce technology and cyber risk. While it is difficult to eliminate shadow-IT completed from an organization, these business-led technology projects should at least be required to adhere to the same policies and standards as every other platform in the company.

DEVELOPER INFRASTRUCTURE

When applications are designed and developed, data is required. Developers stand up and shut down environments constantly to facilitate development and test processes, often leaving in place pieces of infrastructure for years as part of application support processes.

While in most companies, the storage of Personally Identifiable Information (PII) in non-production infrastructure has been tightly controlled for years, there is still a lot of sensitive information that doesn't contain PII stored in development and QA databases. Production data is also often partially or fully replicated into non-production copies that rarely have the same levels of cyber control.

Inventories of sensitive and confidential information need to be extended to include non-production copies, and policies and procedures updated to ensure that the movement of information from protected to non-protected formats as part of the development process is understood and controlled.

PUBLIC CLOUD

When used correctly, the public cloud (Amazon AWS, Microsoft Azure and Google Cloud) can be a very powerful tool that drives down computing infrastructure costs while creating competitive advantage. Yet many organizations still don't require a team that wishes to leverage the public cloud to go through the central cloud engineering and cyber security teams before turning on infrastructure.

It is critical that central standards be established and adhere to whenever the public cloud is used by an organization. If the near constant public reports of un-encrypted, open file buckets and databases on the various cloud providers, often containing very sensitive corporate information is any indication, this is not the case in many companies and creates an area of significant cyber risk.

ORPHANED APPLICATIONS

When an acquisition is first announced, there is a flurry of activity between the acquiring organization and the company being bought. Email systems are combined, networks are connected and databases are loaded with new information. The usual approach is that the acquirer migrates key platforms to their standards with the intent of shutting down duplicate applications brought by the company being acquired.

Yet sometimes these applications don't actually get shut down quickly and because they are intended to be end-of-life, they aren't subject to comprehensive cyber audits and controls. What then happens is these orphan systems, which are often full of sensitive information, hang around for months or years, creating a cyber risk that only grows over time as technology ages and upgrade patches are not applied. This situation can also be created internally when applications are replaced, but the legacy platform is kept running for any number of reasons.

Orphan applications need to be identified and shut down. The excuse that keeping a legacy application running because "it doesn't cost that much" or "we might need to access the information it contains" is no longer valid when the cyber risk created by these orphans is considered.

HIDDEN APPLICATIONS

Every company has applications that contain data so sensitive that they are only accessible by a very small number of people. Examples include anti-financial crime Suspicious Activity Reporting (SAR) platforms and systems that prepare and distribute Board reports. Yet these platforms can often be overlooked as part of cyber risk review processes because so few people actually use them, even though they contain some of the company's most sensitive information.

Most large corporations have thousands of applications, and even mid-sized companies can have 100s. It is important to establish an inventory of all applications, the data they contain and most importantly, their sensitivity, irrespective of the number of users how access them, or how often they are used.

TAKING ACTION

In order to comprehensively understand your cyber risk, it is critical that a business process view is also considered, so as to surface hidden risks that may not be well understood when only asset and threat vector evaluations are performed. Only then can cyber risk be comprehensively managed across the entire organization. Practically, there are four key actions we recommend:

ACTION POINT #1:

- Know what user capabilities are out there across your organization- For End-User Computing and robotic applications, a key first step is to understand the cyber risk that these create for your organization, then to create an inventory and understand how they are being used. The second is to identify all the applications that contain sensitive or critical information (often labelled the 'crown jewels') and ensure there are limitations on the ability for EUCs to access them directly, or large blocks of information to be extracted from them and moved to EUCs.

ACTION POINT #2:

- Apply the data related controls where they matter - It is essential to understand and ultimately inventory the classes of underlying data being called upon and processed by business intelligence tools and ensure the right controls are in place regarding the capture and distribution of the data; be it in raw form or processed. This requires an understanding of which data is sensitive (or potentially attractive to bad actors) in such classes as Non-Public Information (NPI), Material Business Information (MBI) or which collectively represent 'crown jewels' of the enterprise.

ACTION POINT #3:

- Build a data security mindfulness culture - Again, dealing with datasets that are sensitive and potentially valuable to outside parties requires the application of due controls and a positive degree of education by the enterprise regarding data security mindfulness. Where data analysts are aware of the sensitive nature of the data they are privileged to access and process, they are much more likely to take disciplined steps in the handling of such data.

ACTION POINT #4:

- Establish the right base of knowledge about your IT assets and keep this current - Essential to protecting data and reducing or mitigating cyber risk is a clear understanding of the technology landscape and componentry through which data is sourced, processed and distributed. What is unknown is difficult to protect. There are many CMDB (Configuration Management Database) tools available to help keep track of organization assets. The key here is to have the accountabilities and discipline in place to maintain an asset management arrangement to use this effectively combat cyber threats.

Effectively evaluating a company's cyber risk is extremely difficult. It requires establishing a comprehensive inventory of technology and data assets, understanding key process and workflows and considering where trading business flexibility for increased cyber risk is appropriate and acceptable within the company's overall risk appetite.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.

OLIVER WYMAN