10 Cybersecurity Risks Most Executives Miss

Whitepaper by Bill Sheridan

Program Manager for the Security Practice at TBConsulting

TBCONSULTING
TECHNICAL AND BUSINESS CONSULTING, LLC

EXECUTIVE SUMMARY

While some may see cybersecurity as a black art, it is not and cannot be invisible. Executed properly, cybersecurity has an impact that is visible throughout your entire organization — even, and perhaps especially, in your Boardroom. In this whitepaper, we expose ten distinctive and visible red flags that may indicate important deficiencies in your organization's cybersecurity posture. For each red flag identified, we recommend initial actions to help you validate potential problems and start down the path toward resolution.

Without the practitioner's ability to peer into the shadowed digital corners where attackers lurk, how can a business owner or C-Level executive get a feel for the level of cybersecurity risk they are accepting?

INTRODUCTION

Reflecting on the cybersecurity landscape of the past few years — the mega-breaches and devastating data leaks — it's obvious that cybersecurity has become an intractable issue you and your Board simply can't afford to ignore. In fact, in November 2018, Forbes rated cybersecurity and big data as the **number one business priority for leaders** over the next three years. With **the cost of a single breach estimated at an average of $2.2 million** for small and midsize businesses (2017 Ponemon State of Cybersecurity in SMBs), cybersecurity can have a very real impact on your company's survival.

But it's much more than that. When you are hit by cybersecurity incidents, it weakens your competitive edge. It's difficult to compete, maintain efficiency and deliver on your value proposition when your key people are locked in combat with malware or cybercriminals. Effective cybersecurity actually represents an opportunity to maintain, or even **gain** a competitive advantage. For these reasons, it's important to understand and provide oversight of the current state of cybersecurity in your enterprise.

But how can a business owner or C-Level executive, gain awareness of the level of cybersecurity risk they may be unwittingly accepting?

Surprisingly, it's easier than you may think. Today's cybersecurity teams can no longer afford to spend time trying to seal breaches in the outer walls. Intruders have become more savvy, carrying out direct attacks less and less often. They've broken free of the data center and ranged out to threaten partners, staff, and even customers. These cyber-attacks aren't always aimlessly malicious—they are often focused on stealing money. (see Figure 1). More modern threats such as social engineering, email spoofing, phishing, and malware, aren't effectively addressed with tools or ideas from a decade ago. Cybercriminals are stealing data and dollars today by exploiting human mistakes, and these are problems that can't simply be patched.

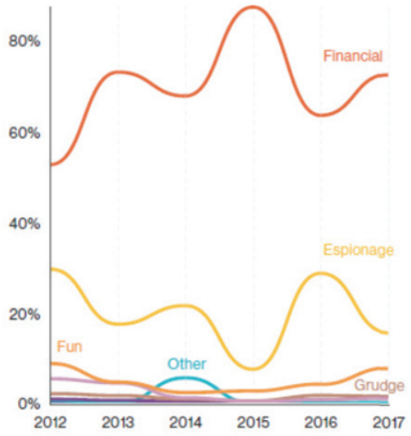


Figure 1

The good news? There are visible indicators that can help you determine if your business might be at risk. They act as a red flag, making it easier to take action, ensuring that your organization is less vulnerable.

In this whitepaper, we discuss 10 indicators to look out for in order to reduce the risk of an attack.

CONTENT

Red Flag #1 Your visibility and special access to systems leaves you vulnerable to cybercriminals

You are a leader whose decisions add value, minimize risk, and create opportunities for your employees. There is little doubt that you are highly visible inside and outside your organization. So why shouldn't your access to company systems and information be special?

To put it simply, that sort of access doesn't just bring exclusivity, it also opens you to threats. Your stature makes you noticeable, and in the eyes of a hacker, you have a big red target on your back. Your authority and access will unlock data (and ultimately dollars) for criminals, just as easily as it does for you. By assuming your identity within your systems, or even posing as you in your human processes (via spoofed emails), an attacker can force your business to work for him.

There are several common ways cybercriminals will expose vulnerabilities of highly visible targets:

- Phishing Attack
- Spear Phishing Attack
- Whaling Attack

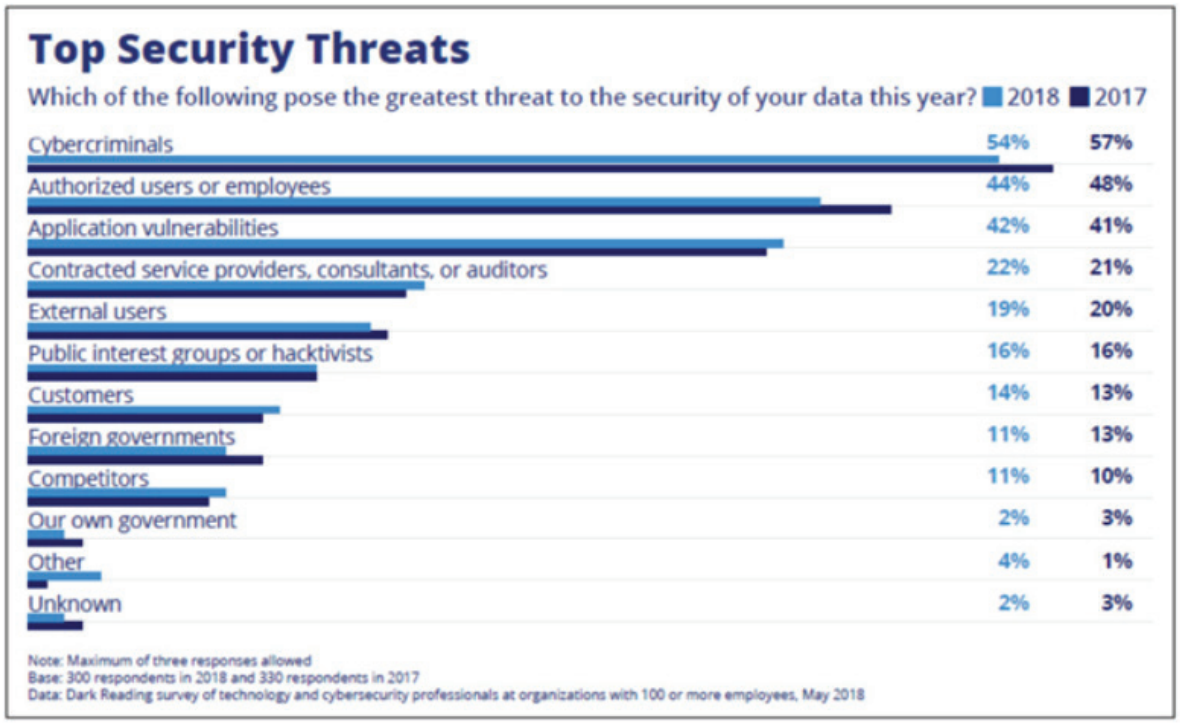
Phishing Attack

In a typical phishing attack, a cybercriminal casts a wide net, simply throwing baited emails into your environment and waiting to see what he pulls up in the haul. The emails may look like invoices, a note from a friend, or even a communication from the HR department. Once the victim clicks on a link or opens an attachment, digital pandemonium ensues. The severity of the damage depends on the access privileges of the user within the system. The amount of access, the greater risk there is of damage and theft.

Spear Phishing

Attacks Cybercriminals know they can steal more with targeted attacks, so they attempt this more direct style of infiltration

In **Spear Phishing Attacks**, cybercriminals look for a weak spot in your processes and then target the unfortunate individual occupying that space. In this case, a cybercriminal might gain access to emails that allow them to identify both the CFO and an accounts payable clerk. Then they could send the victim a spoofed email that appears to come from the CFO, directing the AP clerk to make a bogus payment to the criminal. This attack and the next one we discuss are so focused that according to INFOSEC Institute, 77% of Spear Phishing attacks target 10 email inboxes, and 33% of them focus on just one email inbox.



Whaling Attack

But you are a big fish, worthy of focused individual attention. In a targeted attack called Whaling, the criminal aims for a target with influence and authority that they can use to do real damage. In TBC's experience, this has often been the CFO.

In a Whaling Attack, the cybercriminal may send a tailored, personalized message asking their target to take some action. The note might appear to be from someone the victim trusts explicitly. The attacker may ask the victim to open and review an attached invoice that is actually malware. They may send the target to a website that will steal their password. Or they may pick up other contact names and imitate the executive in an email, using their authority to steal whatever they can. Regardless of the tactic used, the resulting damage will be in direct proportion to the executive's privileges on targeted technology, and their influence over targeted people.

What is the potential impact of Whaling and Spear Phishing? This varies considerably, but Spear Phishing is all about big money. We are aware of cases where the potential losses range from $50K to over $1 million. In 2017, Ubiquiti Networks lost $46.7 million, so this is a risk worth managing!

Recommended Action

To effectively manage this risk, it is best to assume you will be compromised. Cybersecurity experts emphasize that every element within your IT systems (and each individual is an element), should have only the minimum amount of access that it needs to do its job.

Have your IT staff provide you with an account that can be used for exploration and removed or disabled later. and make it clear to the IT team that none of the other executives at the company should either.

Red Flag #2 You Haven't Taken End-User Security Training

Not long ago, TBConsulting became aware of a company that suffered a devastating malware attack. An employee with nearly unlimited systems access double-clicked on an email attachment and most of his company's files were immediately and irreversibly encrypted. Backups were damaged and efforts to pay the ransom did not return access to the files. The damage was crippling and took weeks to undo.

We can only estimate the cost but the **Ponemon Institute estimated the average cost of a data breach for a small to mid-sized company at $2.2 million.**

What went wrong? Of course, this person shouldn't have been opening these types of emails using an account with such broad access privileges, but more importantly: the user did not, and had not been trained to recognize the potential danger present in emails.

Recently, **87% of executives around the world cite untrained staff as the greatest cyber risk to their business**, according to research performed by ESI ThoughtLab, in conjunction with Willis Towers Watson

Keep in mind that cyber threats lurk in dark corners throughout the IT landscape. Phishing, of the sort we mentioned above, is just one type of risk. The only way to provide employees with the knowledge and mindset they need to recognize and avoid most threats and risks is through formal security training. Employees should be expected to take cybersecurity training at least annually, pass a test at the end of the training, and agree to abide by what they have learned.

Recommended Action

To close this gap, work with your CISO and HR leadership to institute ongoing, mandatory security training for all employees. Take the training yourself and work collectively with your Board to reinforce its value and critical importance.

Not sure where to start? Feel free to contact us and we'll happily point you toward a few options.

Red Flag #3 You're Not Talking to Security Directly

Most of your IT department is focused on providing services using a combination of infrastructure and applications that deliver the support and value you expect. But Security is different. The service that Security delivers is risk management, and the management of risk is often the Board's responsibility. If the news from your Security team is filtered through one or more middlemen, you may not be getting the data you need to make critical decisions.

But that's not the only reason you should be talking to Security. In a recent case of Spear Phishing, a cybercriminal gained access to a company principal's account, then monitored his emails. Using a "spoofed" email (a note that appeared to be from the principal, but was in fact from the hacker), the criminal directed an employee to send a significant payment directly to him. The resulting loss was in the tens of thousands of dollars.

From a security perspective, perhaps the most remarkable thing about this incident is that it is not remarkable at all. Any security professional or security-savvy employee could have seen this coming a mile away. Ask yourself, in what other context would anyone authorize payment in the tens of thousands of dollars to a previously unknown vendor, without so much as a verified signature or personal confirmation?

Your security team needs people with the motivation, skills, and time to ensure that configuration issues, like the one we just mentioned, are identified and corrected. They need to understand the journey from your current at-risk state, to a lower-risk future that is both usable and affordable. And they need to communicate that information directly to you in language and metrics that are relevant to your business.

The Board should manage risk, drive changes to your business culture, or obtain people and tools without a mandate and budget. But Board members need Security's knowledge and experience to understand the risks and the action necessary to manage them. If your cybersecurity team is not banging on your door, or if cybersecurity risks are buried deeply in IT budget requests and business justifications, you may just be seeing Red Flag #3.

Recommended Action

Schedule a meeting with your CISO or cybersecurity team and the appropriate Board members. Ask them to evaluate your current security posture or bring in an outside team that can. Encourage honesty and transparency and ask for the bad news with the good.

Require that IT provide the Board with regular cybersecurity reports, detailing what's been done and what needs to be done. And remember, you don't have to leave this exclusively with your CFO, CTO, or CISO. Many organizations set up security subcommittees within the Board.

Red Flag #4 You Get a Lot of Spam

A 2018 survey of 2410 IT and cybersecurity decision makers, run by security software maker Tenable and the Ponemon Institute, revealed the number one attack experienced in the prior 24 months by 67% of respondents stemmed from "a careless employee fell for a phishing scam that resulted in credential theft."

Most spam is annoying but relatively harmless. Think of it as a wolf in sheep's clothing. Spam is an indicator that your email systems are not filtering effectively and, sprinkled among those sheep, there may be the occasional wolf. It's a simple question of exposure: the more faux sheep, the greater the risk that you or a member of your team is going to get bitten by one of those hidden wolves.
Amid the deluge of emails you receive, you may feel you have become adept at identifying spam and phishing attempts. But some emails are sophisticated and effectively mask their intent; they may contain links that can download, install, and unleash malware that can use your access privileges against you.

If your inbox is full of spam, it's likely that your organization is also receiving a lot of spam which increases the likelihood of someone in the organization being exposed to phishing attacks.

Recommended Action

Direct your IT team to review their email filters and tighten up the controls. Ask them if emails are routinely accepted from all domains globally. If you run a manufacturing firm in Muncie, Indiana, do you really need to accept emails from Vladivostok in Russia?

Instruct your IT and security teams to recommend the right balance of spam filtering for your company. Allow yourself and users time to adapt to the new set tings, and direct IT to provide training so that legitimate data is not lost.

Red Flag #5 The IT Department Is in Chaos

While the majority of IT organizations sometimes need all hands on deck and late nights can be part of the role, if long hours and frenzied activity have become regular occurrences, there's a problem. When IT is routinely absorbed in keeping its head above water, and responding to crashes, its best people may not be thinking about less visible, but essential, elements of work such as IT Security.

Over time, this deferred, but important, work builds up as technical debt, while anything in the spotlight is given heroic attention. This is a poisonous state for any IT organization and often leads to serious cybersecurity shortfalls that turn your environment into a rich hunting ground for hackers and cybercriminals.

So, if you see your people grabbing IT staff and dragging them off to their desks for ad hoc support sessions, or you're signing off on an enormous bill for midnight pizza runs and Red Bull™, you may be seeing signs of Red Flag #5.

Recommended Action

Not long ago, IT was considered an expense, nothing more than a cost to be minimized — but that short sighted view starves strategic objectives and undermines your company's growth.

Review your IT budget and spend with your financial team to ensure you are adequately funding strategic objectives such as security and digital transformation... Top analyst firms can provide information around typical IT spending, generally as a percent of revenue, for most industry sectors. If your spending falls far short of the norm, it's an indication that IT needs more attention.

Assign an internal or external resource to evaluate priorities, bottlenecks, and workflows. IT needs to know how to control, prioritize, and resource its work to align with business needs, including cybersecurity. If your budget allows and you can find the talent, build an internal dedicated security team. But security people and tools can be expensive and in short supply, and the time to build processes, configure systems, establish integrations and connections with the business can lengthen your exposure to risk.

To avoid these obstacles, consider engaging a Managed Security Services Provider (MSSP). MSSPs have the tools and processes already built, and they divide the cost of maintaining expensive security teams and infrastructure over many clients, reducing the cost to each client while maintaining effective services. The right MSSP can provide you the security you need without delays or excessive spend.

Deficiencies in Your Organization's Cybersecurity Posture

These next 5 red flags may indicate significant deficiencies in your organization's cybersecurity posture that expose your business to serious risk. For each, we propose action to help validate the potential problem and start down the path toward resolution.

Red Flag #6 No Annoying System Restarts

In cybersecurity terms, a security weakness in software is called a Vulnerability. Newly discovered vulnerabilities are referred to as Zero Day Vulnerabilities and are not always immediately dangerous. It's not that these lack potential, it's just that it takes time for hackers and others to figure out how to use these vulnerabilities to gain access to your data.

Once discovered, often only the most skilled cybercriminals and hackers can exploit a newly discovered Zero Day Vulnerability. After making the discovery, they develop a method known as an Exploit. If the cybercriminal shares the Exploit, it will be built into the next release of major hacking tools, and anyone with knowledge (and funding for the tool) will be able to use the Exploit to attack your business.

Software developers are charged with creating fixes in the form of new code, known as patches, that are applied to operating systems and applications to manage against these new Exploits. Ideally, your IT team uses automated software to distribute patches to end-user devices (like your laptop) and to other devices within the environment. If you, or another user, turn off automatic updates to avoid pesky reboots, vulnerabilities are never patched. That means your system is at an ever-increasing risk of compromise as time passes.

So, do you remember the last time your computer interrupted your work or delayed your system startup to apply updates? If you have to think back more than a few weeks, you may be seeing Red Flag #6.

Recommended Action

Consult with your IT team to ensure updates are consistently being applied to your environment. If not, remind them that you need to be protected as well, or better, than anyone else.

If the lack of updates applies to all systems in your environment, you may have a larger issue. It's not enough to apply current patches, as older vulnerabilities can be very dangerous. Direct IT to perform a security assessment on your environment to reveal the extent of your vulnerabilities and help build a roadmap to a safer environment.

Red Flag #7 You don't see the 'S' in HTTP (S)

It's all about the S. If you go to the login page of your website or internal apps, you can look at the address bar, at the top of your browser window, and see the Uniform Resource Locator (URL) your browser is accessing. For example, the URL for logging into your Google account: https://myaccount.google.com/

You'll notice that the URL begins with https, which stands for Hypertext Transfer Protocol Secure. The "S" at the end tells your browser to use a technology called Secure Sockets Layer (SSL) to encrypt all communication going out over the network. With SSL, only the computer you are connecting to can read the information that you are exchanging. If it begins with http:// (no S), your information is going across the network, and perhaps the Internet, in a clear readable format to cybercriminals and hackers.

This means that you, as a CXO, can tell at a glance if your network communications are secure. Packet sniffers are a favorite diagnostic tool among IT professionals, but also one of the first tools used by hackers. Given its power, it's not surprising how ubiquitous packet sniffing software is today. Right now, you can download packet sniffers for your PC or your cell phone and read the data flowing through your IT network. If your team is not careful, cybercriminals can use packet sniffers to see your login IDs and passwords, client data, or even transactions with external companies.

And the damage isn't necessarily limited to accessing your network via stolen login IDs and passwords. An attacker could potentially glean sensitive data (e.g., health records or credit card information) directly from network trac as well. This could prove very damaging to your business, both in terms of direct financial impact and a tarnished reputation that leads to loss of client trust.

Recommended Action

Consult your IT department and/or development team and make it clear that login information should never go over the network, even internally, without encryption. Ask them about client data as well. If client data is traversing the network in clear text, that needs to be changed immediately.

In addition, websites outside of your own may ask for your credentials without using HTTPS. If a site you commonly visit accepts passwords using HTTP, refrain from logging into the site until its owners can implement proper security.

Red Flag #8 You Still Have Systems Running Windows XP

The adage "if it ain't broke, don't fix it" may be good advice for an old milling machine or press, but it is poor advice for IT equipment. If you have equipment running Windows XP or any other version of unsupported software, it's already "broke!"

When an operating system or other software reaches end-of-life, its developers no longer fix bugs or patch vulnerabilities. Hackers and cybercriminals exploit those bugs and vulnerabilities, causing your software to become increasingly vulnerable. Like an old, unmaintained bridge, the structure may appear secure, but it is rotting from the inside; its weaknesses may not be discovered for a very long time.

An attacker will discover it, exploit it, and use it to gain access to your environment. Depending on the severity of the exploit, the skill of the attacker, the condition of the rest of your environment, and many other factors, the damage may be minimal, or it may be catastrophic.

The story is similar with old hardware. Various hardware components that make up your PC also contain their own code, called firmware, that can contain vulnerabilities as well. The probability that someone has found and can exploit these vulnerabilities increases with the device's age.

But firmware isn't the only problem. Typically, older hardware will not have the resources to run new software while maintaining a reasonable level of performance. The larger the age gap, the more likely it won't run new revisions of your software at all.

In time, it becomes the sort of weakness attackers can exploit to gain a foothold in your environment. So, when you walk past those ancient, un-scrubbed machines on the production floor, or if you see a billing clerk working at a machine that still has a floppy disk drive, you may be seeing Red Flag #8.

Recommended Action

If you've got old equipment and software running in your enterprise, it's time to think about upgrades or consider new solutions. Windows XP hasn't received security updates since April 2014. Windows Vista reached the end of its supported life on April 11, 2017. Windows 7 will no longer receive security updates as of January 2020. If you are still using either of these operating systems, you must start thinking about protecting your enterprise now.

Engage a security professional to perform a vulnerability analysis. Evaluate the results considering increased risk of attacks, diminishing support capabilities, and the potential cost of custom coding. This will provide the insight to decide if the cost of replacing the old technology can be justified.

Red Flag #9 Software is a Personal Expense

Many environments, particularly in R&D, permit the acquisition of various advanced software and tools to support cutting edge techniques for research and analysis. In an R&D lab, this sort of freedom is essential, but can lead to a huge problem. It creates a proliferation of multiple revisions of the same software installed on different machines scattered about the lab.

It results in the existence of several tools with huge functional overlaps, each of which require learning and understanding from the user, and expensive support contracts. And, some users may put their software purchases on their personal credit card. This creates a set of features and vulnerabilities that may be neither understood nor controlled.

While old versions of software can conceivably deliver different results than new, older versions are always less secure. Since IT ostensibly has no visibility or control over software loaded on such machines, they also may lack transparency regarding the existence and whereabouts of critical research data contributing to questionable security and reliability. The risk of data corruption, loss, or theft in this scenario is very real.

If you see large personal or departmental expenses for software purchases, or if you are personally capable of downloading anything and installing it on your own machine (see Red Flag #1), you may be seeing signs of Red Flag #9.

Recommended Action

Consult your IT leadership team to assess their control over the installation and maintenance of software in your environment. If they are not exerting this control, your firm could be exposed to unnecessary expense and risk.

A security assessment may help determine the degree and the severity to which open download capabilities may open your enterprise to attackers. Part of the output of that assessment should be a list of the groups with critical vulnerabilities and a roadmap for resolving them quickly.

Essential tools should always be purchased with support so that they are frequently updated, and such that your team has access to the developer's support services. If you have old software that is no longer supported but absolutely must remain in use, IT should be empowered to work with the user/department to find a suitable replacement, or to isolate the software from the remainder of the environment.

Red Flag #10 You Use a USB Drive

Time was that the biggest threat the enterprise faced was external — the hacker, the Hacktivists, or the "script kiddy" using free malware to poke at your systems. But today, with cybersecurity issues in the spotlight, motivated insiders know that they can hurt you or make money from you by exploiting their access to your systems and information. It's never been more important to control that access and monitor its use.

A simple test to expose your risk is to plug an encrypted USB drive into the port on your laptop, find some sensitive and high-volume data, and download the data directly onto the drive. This should trigger a phone call from IT to determine if you downloaded the information. If your IT organization is not capable of detecting exfiltrations of this sort, you may be seeing evidence of Red Flag #10.

This is a complicated issue to evaluate. Allowing the removal of data from your environment in any format is inherently risky; balancing employee productivity with risk management is challenging. Controlling risk in external environments, such as employees' homes, is very diffcult; requiring encrypted hard drives, stipulating systems are turned off when not in use, securing wireless signals and controlling production of additional copies of data may exceed the capabilities of your IT team.

Further, there may be risks and implications if the data is subject to HIPAA, PCI, or other regulatory requirements.

If you allow data to leave the building, IT should have controls in place that govern who can access that data and how. But in addition to this, IT should have a published policy regarding mobile devices, removable devices, and remote access. Every employee in the enterprise, including you, should be aware of and trained on those policies. And if any employee in the company is copying data to removable devices, or even to locations across the Internet, you need to be able to detect it. If not, you're probably getting a good look at Red flag #10.

Recommended Action

First, don't be rattled if you didn't get a phone call from IT when you performed the experiment above. Although it's a critical issue, this is a widespread problem and one that businesses of all sizes and sorts are struggling with today. It's not going to be solved overnight, but it represents a significant security risk and needs to be on IT's radar.

The risk is high. Mobile devices such as phones and tablets have huge storage capacity and make it possible for users to walk out your front door carrying stunning amounts of your data. In 2019, cell phones are available with installed memory up to 1.5 TB. The largest USB flash drives store up to 2 TB of data. Even an employee on his Internet connection at home can download and copy data at rates up to 2 Gb per second.

Authorized people still need access to the data. The only way to protect yourself from authorized people performing unauthorized downloads is through security monitoring. With the right tools and skilled people, you, or a qualified Managed Security Services Provider (MSSP), can identify data exfiltration in progress and can even stop the event automatically.

Advanced monitoring services can do even more. For example, File Integrity Monitoring (FIM) can detect when critical files are modified, preventing the insertion of malware and viruses. More advanced monitoring can also apply an artificial intelligence tool called User and Entity Behavioral Analysis (UEBA).

By learning what is normal in your systems and users' behavior, this can even flag and alert on unusual behaviors (like an employee logging in at 3:00 AM and downloading sensitive data). UEBA gives you the ability to detect fraudulent activities, and potentially even shut them down before data is lost.

Conclusion

IT security is complex and critical. The red flags noted above can alert you to potential issues and are good conversation starters for connecting with your IT team. But if you see one or more of the red flags listed, it doesn't necessarily mean that your team is unaware of the problem, or that they're being careless, or incompetent. It means that there's a barrier between your people and a stable, secure environment. It's in your best interests to make sure that any such barrier is removed, and that IT has what it needs to keep your business secure.

If this whitepaper gave you cause for concern, it may be time to consult with your IT team. Ask them if they have compensating controls that you're not seeing. If they confirm the issues, give them the mandate, the help, and the resources they need to formulate a plan and get your security under control, before someone does some damage. If they need additional time, manpower, or skills reach out to professionals for assistance. There are many reputable ISSPs who can provide you with what you need.

Questions or Comments?

Bill Sheridan is the Program Manager for the Security Practice at Technical & Business Consulting (TBC), an MSSP located in Scottsdale, Arizona. In his role, he encounters client security issues regularly and has become a strong proponent of the use of eective communication between security and the Board. Bill welcomes your thoughts and ideas, and can be reached at the following email address:

wsheridan@tbconsulting.com