7 Cybersecurity Red Flags Executives Often Miss

TBCONSULTING

EXECUTIVE SUMMARY

While some may see cybersecurity as a black art, it is not and cannot be invisible. When appropriately executed, cybersecurity impacts your entire organization — even, and perhaps especially, in the C-suite. This white paper exposes seven distinctive red flags that may indicate critical deficiencies in your organization's cybersecurity posture. We recommend initial actions with each red flag to help you identify potential problems and the steps toward resolution.

The cybersecurity landscape of mega-breaches and devastating data leaks makes it abundantly clear that cybersecurity is an issue that your organization cannot afford to ignore. The National Association of State Chief Information Officers (NASCIO) reports that cybersecurity remains the top priority for 2022. Moreover, with the average cost of a data breach at $4.24 million 2021, the long tail costs of an attack include reputational damage, business disruption, lost sales, specialty IT remediation, and fines – all of which can follow an organization for years.

If your company suffers a cybersecurity attack, it weakens your competitive edge. During the disruption, it becomes difficult, or even impossible, to maintain productivity and deliver on your value proposition. When your key people face critical decisions on how to recover from an attack, their focus is not on growth and profitable initiatives. To best secure your organization's long-term goals, it vital to understand the current level of your cybersecurity maturity and learn how to implement cybersecurity solutions that will protect the future of your business.

While your security teams are firefighting to keep your network and systems protected, they are too busy to address the risks of careless employees and increasingly sophisticated cyberattacks. With human error accounting for 95% of all data breaches, today's cyber criminals steal data and dollars by exploiting human mistakes through social engineering, email spoofing, phishing, and malware. Executives must take responsibility for implementing cybersecurity awareness training, funding cybersecurity staff and tools, and implementing policies that protect the organization.

But how can a business owner or executive team accurately assess the level of cybersecurity risk the company faces? There are visible indicators that can help you determine if your business might be at risk. They act as red flags making it easier to take action and ensure that your organization is less vulnerable. In this cybersecurity white paper, we discuss seven of those red flag issues and for each we also discuss a recommended course of action.

CONTENTS

Red Flag #1
Security is just a line item on your budget

Cybersecurity cannot be relegated to a single line item in your budget. Cybersecurity touches every component of your organization – from protecting confidential HR files and intellectual property, production and distribution, and applications and data, all of which tie into your business's success. But how can you accurately identify and track the multitude of devices, applications, data, and users on your network that need protection? The answer is to use a cybersecurity defense matrix that imposes a framework across your organization to identify risk and measure security success. The focus on measuring security risk is essential to ensure that you are getting value from your security spend. The measurement is not only in dollars but in security coverage and the reduction of risk.

The executive's role is to provide strategies for growth, costs, marketing, and profitability. Why should security be any different? If your business has not already incorporated a security strategy, how can there be an expectation of success?

The frightening reality is that most businesses do not have a strategy around security. Sure, executives approve budgets for tools, staff, and software, but those things are usually siloed by department, without the benefit of an overall security strategy. For example, during the panic mode imposed by a breach, the tendency is to spend money on a quick fix without considering the impact of adding additional tools to the environment. Often, the more serious the breach, the more cash thrown at the problem.

Recommended Action:

Treat cybersecurity just as you would every other aspect of your business. Take the time as an organization to develop a coherent and inclusive security strategy where you can determine your acceptable risk and measure your success against a framework. Planning out your security strategy will ensure that you have the proper people, tools, and budget in place to protect your organization.

Red Flag #2
Your visibility and special access identify you as a target for cybercriminals

As an executive leader whose decisions add value to the business and create growth opportunities for your employees, your visibility can become a hardship. There is little doubt that your position is reflected inside your organization and broadcast to the outside world through social media, award coverage, and published interviews. Cybercriminals are also taking notice of you and know that your unique access to company systems and information is extensive and confidential – and they want your access.

The exclusivity of your position can leave you vulnerable to cyber threats, and your name used against your employees for successful phishing or social media cyber-attacks. Your authority and access will unlock sensitive data for criminals just as quickly as it does for you if they find their way into your network. By assuming your identity within your systems or posing as you via spoofed emails, an attacker can manipulate your business and infringe upon your successful enterprise.

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 user's access privileges within the system—the more significant the access, the greater risk of damage and theft.

Spear Phishing

Cybercriminals know they can steal more with targeted attacks, so they attempt a more direct infiltration style. In spear-phishing attacks, cybercriminals aim for specific accounts or departments and target an unfortunate individual. For example, cybercriminals might gain access to emails that allow them to identify both the CFO and an accounts payable clerk. They then 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. Spear phishing is very successful – up to 74% of data breaches begin with a spear-phishing email.

Whaling Attack

As the gatekeeper in your organization, your special access makes you a high-profile fish worthy of focused individual attention. In a targeted attack called whaling, the criminal aims for a target with influence and authority who can unknowingly assist them in causing significant damage. In TBC's experience, this target has often been the CFO.

In a whaling attack, the cybercriminal may send a tailored, personalized message asking the target to take some action. The note might appear to be from someone the victim trusts explicitly. For instance, the attacker may ask the victim to open and review an attached invoice that turns out to be malware. Or they may send the target to a website that will steal their password. Another method is to obtain contact names, imitate the executive in an email, and then use his or her authority to steal whatever is available for the taking. Regardless of the tactic used, the resulting damage will be in direct proportion to the executive's privileges on targeted technology and his or her influence over targeted people. What is the potential impact of whaling and spear phishing? The result varies considerably, but whale phishing aims to steal big, so it is well worth your time to manage this risk.

Recommended Action

To effectively manage this risk, assume that your company will be compromised at some point. Cybersecurity experts emphasize that personnel within your IT systems should have only the minimum amount of access necessary to perform the assigned job.

Red Flag #3
Cybersecurity awareness training is not part of your workplace culture

The pandemic that forced employees to dispatch to offsite locations quickly and the extension of hybrid work situations has been a boon for cybercriminals. Remote and hybrid workforces, without the luxury of consistent, in-office security controls, company equipment, internet access, and network access, have often resorted to using their own devices and downloading rogue software to get their work done.

When working remotely, workers need more controls, not less. End-users must become 'security aware' and executives must build a culture of cybersecurity awareness which become an indicator of the organization's cybersecurity health. But with the heightened levels of activity at home, employees are often distracted and can lose their awareness edge.

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. As a result, 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.

End-User Security Training

What went wrong? Of course, this person should not have been opening these emails and should not have had such broad access privileges. But, more importantly, the user had not been trained to recognize the potential danger present in emails.

End-User Security Training, also known as Cybersecurity Awareness training, is essential for your hybrid workforce. A staggering 69% of employees, who lack the training to avoid engaging with a suspicious email, could be vulnerable to click-bait schemes and invite a cyberattack into your systems.

Keep in mind that cyber threats lurk everywhere 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 dangers is through formal security training. Therefore, company policy should require cybersecurity training for all employees on a routine basis. Management should expect that all employees will attend the training, pass the test, and abide by the cybersecurity protocols that 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 and make it part of your workplace culture. Take the training yourself and work collectively with your leadership team to reinforce its value and critical importance to the health and success of the company.

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

Red Flag #4
You are not talking to your security team directly

Your IT department focuses on providing services and delivering infrastructure and applications to support your business. But the IT security team is different. The IT security team shares the responsibility of risk management with senior leadership. If your IT security team is not speaking directly with management, you may not be getting the data you require to make critical decisions. It would be best if you worked together to map out the journey from your current at-risk state to a lower-risk future. The security team should communicate relevant metrics that will inform business strategy and align with your budget.

But that is not the only reason you should be talking directly to your security team. It would help if you were building a trust-based relationship with your security team to know your voice and quickly identify any suspicious behavior in your accounts. Suppose an executive's email account is compromised. Do you have standard protections in place that can stop unverified payments to an unknown vendor and require prior authorization, a verified signature, or personal confirmation from the executive before sending payment?

The executive leadership team cannot manage risk, drive change, mandate an appropriate budget, or procure the right resources and tools without input from the IT security team. Executives should rely on the knowledge and experience of the security team to understand the risks and the actions needed to manage them. So, if your cybersecurity team is not banging on your door, or if security falls deep in IT budget requests, that is a red flag that you should not ignore.

Recommended Action

Schedule a meeting with your CISO or cybersecurity team and the appropriate members of the executive leadership team. Ask your internal experts to evaluate your current security posture or bring in an outside team if necessary. Encourage honesty and transparency in the assessment and clarify that you want to discuss all the news-the good, the bad, and the ugly.

Require that IT provide management with regular cybersecurity reports detailing the progress of changes made and planned for the future. And remember, you do not have to leave this exclusively with your CFO, CTO, or CISO. Many organizations set up security subcommittees within the Board or management team.

Red Flag #5
You get a lot of spam

Most spam is annoying but relatively harmless. Spam is an indicator that your email systems are not filtering effectively. But the critical issue is exposure: the more spam you receive, the greater the risk that you or a member of your team will be exposed to the type of spam that turns out not to be harmless.

Amid the deluge of emails you receive, you may feel you have become adept at identifying spam and phishing attempts. But cybercriminals are becoming more sophisticated and can effectively mask their intent; they may contain links that can download or install malware to infiltrate your systems. In addition, if your inbox is full of spam, then it is likely that your colleagues are receiving a lot of spam too, which increases the likelihood of someone in the organization being exposed to phishing attacks.

Recommended Action

The IT and security teams should conduct a thorough review of the organization's email filters and tighten up the controls, as required. The relevant query: Is email routinely accepted from all domains globally? For example, if you are operating a manufacturing firm in Muncie, Indiana, should your employees receive (and open) emails from Vladivostok, Russia?

Direct your IT and security teams to recommend the right balance of spam filtering for your company. Understand that all users will require time to adapt to the new controls. In addition, for these new protocols to be effective, the IT and security teams must provide training to all employees to prevent the loss of legitimate data.

Red Flag #6
The IT department is in chaos

Most IT organizations periodically participate in fire drills or face events that require “all hands on deck.” If situations like those become routine and contribute to a continuously frenzied atmosphere, read that as a clear signal of a problem. When IT is routinely absorbed in responding to crashes, strategic thinkers cannot focus on essential issues like cybersecurity risk management and protecting their workforce.

Over time, deferred work and lack of strategic planning build up as technical debt. And while events continue to receive immediate attention, ignoring mounting technical debt signals a dangerous state for your IT environment. The resulting cybersecurity shortfalls can leave your organization vulnerable to hackers and cybercriminals.

The pandemic was a great differentiator between those companies who were already functioning in the cloud and maintaining cybersecurity protocols within their network and those companies who were wholly unprepared for the move to remote work. IT departments across the globe had to help people connect, scramble for laptops and personal devices, implement safe file sharing, and get people back to work. Everyone was in chaos, but unprepared businesses and those still clinging to legacy infrastructure were most gravely impacted. The length and magnitude of the pandemic have mellowed the chaos, and executives and IT teams can now focus on planning for the future.

Are your IT managers are consistently pulling staff away from long-term projects to handle ad hoc issues, or if funding runs for midnight pizza and Red Bull™ becomes standard protocol, you may be seeing signs of Red Flag #6.

Recommended Action

IT departments and resources are often considered a necessary expense, but few understand how a poorly funded and managed IT department can destroy strategic business objectives. Technical debt undermines your company's growth and increases cybersecurity vulnerabilities.

Review your IT budget with your financial team to ensure that you are adequately funding strategic objectives, such as security, maintaining a hybrid workplace, and digital transformation. Help support and fund the increasingly significant role your IT department plays in cybersecurity and strategic initiatives.

Assign an internal or external resource to evaluate priorities, bottlenecks, and workflows. IT can more easily control, prioritize, and resource work demands to align with business needs if properly funded. An IT team in constant chaos is a liability and will eventually make costly mistakes. If your budget allows, consider building an internal, dedicated security team with clear guidelines, policies, and the ability to implement innovative solutions. Finding the right security talent and tools can be expensive and are often in short supply. It takes time to create the processes, configure systems, map out integrations, and find the right people to manage the department effectively.

To avoid these obstacles, consider engaging a Managed Security Service Provider (MSSP). MSSPs have the tools, the people, and the processes in place to implement extensive cybersecurity protection. If you cannot find room in your budget for a fully staffed SOC, you can enjoy the benefits of working with an MSSP to effectively cost share on resources, equipment, maintenance, and infrastructure. Expert security teams and industry-leading tools.

Red Flag #7
Missing those annoying system restarts?

For 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 vulnerabilities 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. They develop a method known as an 'exploit.' If the cybercriminal shares the exploit, it is built into the next release of major hacking tools, and anyone with knowledge (and those funding 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, 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 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 without updates and patches.

Do you remember the last time your computer interrupted your work or delayed your system startup to apply updates? If it has been more than a few weeks, you may be seeing Red Flag #7.

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 everyone else.

If the lack of updates applies to all systems in your environment, you may have a more significant issue. It is 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.

CONCLUSION

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

If this white paper gave you cause for concern, it is time to consult with your IT team. Ask them if they are seeing issues that they do not have time to address and work with them to develop a security plan. Give them the help and resources they need to get your security under control before damage occurs. If they need additional time or security expertise, reach out to professionals for assistance. Many reputable MSSPs can provide you with what you need.

Questions or Comments?

Tyler Edgett is the Security Practice Manager at TBConsulting, an MSSP located in Scottsdale, Arizona. He helps clients navigate complex security issues and has become a strong proponent of effective communication between IT and executive leadership teams. Tyler may be reached at **tedgett@tbconsulting.com**

Click Here for a Quiz to Evaluate your Cybersecurity Maturity