www.pipelinepub.com
Volume 20, Issue 1

Building Your Risk Management and Security Strategy

By: Paul Baird

To operate successfully, companies need reliable, trustworthy, and secure IT to support their processes. For many years, IT was perceived to be necessary as a cost of doing business rather than a means of enabling the business in the first place. This attitude has changed, and today IT is inseparable from how businesses operate. In its *State of Cybersecurity Resilience 2023* report, Accenture found that organizations that closely align their cybersecurity programs to business objectives are 18 percent more likely to increase their ability to drive revenue growth. Similarly, Deloitte's 2023 Global Future of Cyber Survey report found that 56 percent of business leaders ranked greater efficiency as the biggest impact of cyber security investment, closely followed by detecting problems sooner at 55 percent.

At the same time, investments in IT security have grown. International Data Corporationpredicts that global spending on security will top $219 billion in 2023, a 12.1 percent increase over 2022. This is despite economic pressure that has slowed other areas of technology spending. Such spending is warranted, as the Business Continuity Institute's *Cyber Resilience Report 2023*reported that 74 percent of organizations saw an increase in cyber attacks during the last year.

With so much emphasis on technology, and so much to lose if things go wrong, it is no surprise that IT security leaders are under the spotlight of the board. They want to know what risks exist, the potential business impact those risks pose, and how they are being managed or mitigated. More importantly, with so much funding being made available to security teams, boards want to know what specific actions are taking place right now, not in the future, to limit risk exposure.

For chief information security officers and other IT security leaders, increased attention comes with greater accountability as well. For example, the Securities and Exchange Commission filed Wells Notices against members of the leadership team at SolarWinds in relation to the cyber attack the company suffered, signaling it intends to file a civil enforcement action against the

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for distribution or reproduction.

recipients for alleged violations of U.S. federal securities laws. This follows the case against Uber's CISO, who was found guilty of misconduct relating to a data breach that occurred in 2016.

Getting ahead of your board

With all this in mind, it is essential to have a long-term view of your cyber security program in place in order to have any chance of staying ahead of threat actors. Getting business support for your cyber security program is a step in the right direction, but it should not be your end goal; once that backing is secured, attention needs to be focused on results that align with desired, previously agreed upon business outcomes.

The first step is prioritization. Within today's complex digital environments, the many potential issues and challenges that can affect digital assets can make it harder to focus efforts to achieve maximum positive impact. Worse, this reality can be difficult to communicate to board members, who won't want to delve into particular circumstances or challenges. They will want to focus on the biggest risks that might affect the organization and what is being done to mitigate them.

Prioritization of security issues has been a challenge for many years, but can offer the biggest opportunity to counter security risks at the source. For example, in our *TotalCloud Security Insights 2023*report, we found that many cloud security deployments were failing to implement standard security best practices. The average failure rate for AWS deployments around Center for Internet Security benchmarks was 34 percent, rising to 57 percent for Microsoft Azure and 60 percent for Google Cloud Platform. Best practices can effectively eliminate whole swathes of potential threats, but time and resources are required to implement them. By looking at the bigger picture, best practices can be used to mitigate whole areas of tactics, techniques and procedures (TTPs) that threat actors commonly employ.

Similarly, we can look at the issues that represent specific threats to our organizations. In our *TruRisk Research Report* for 2023, we found that 25,228 known vulnerabilities were discovered over twelve months. This is a huge number of issues to consider. Yet only 159 of these issues were actually weaponized with exploit code, and only 93 were actually exploited by malware. Similarly, 539 issues from previous years were exploited by threat actors, and 118 were more than three years old.

What does this tell us? First, security issues can be difficult to fix. The reasons why security fixes don't get implemented are: a lack of awareness that vulnerabilities exist within the organization's infrastructure, or the concern that making a change would break other applications and systems. Understanding these risks and managing them effectively is a bigger issue than simply looking at numbers of potential vulnerabilities that must be managed, so providing the right context to your board over time is essential.

Second, not all issues are created equal. What represents a serious or business-critical risk to your organization may not be a risk at all to another company. Business risks are organic, changing in severity over time due to internal and external factors. For instance, a security flaw that is nothing to worry about on its own can become critical if it can be used as part of an automated attack chain involving other vulnerabilities. Synthesizing all this data, understanding it in context, and applying prioritization to risks over time should help you manage security, remediation, and

mitigation efforts. Lastly, automation is essential to your efforts. Functions such as asset management and inventory and patch deployment should be automated as much as possible to improve efficiency. Your board will want to know how efficient your team is at preventing known issues, and automation will help remediate issues faster. Based on our research,

© Pipeline Publishing, L.L.C. All Rights Reserved.

automation associated with critical applications like Google Chrome, or the most widely deployed operating system, Microsoft Windows, ensures that these applications are patched twice as fast and twice as often as other applications that are lower down the priority list.

Providing information, proving value

Along with improving your team's efficiency around patching and remediation using automation, you should also look at how you communicate with your business about your efforts. It's not enough to be doing the right things in security, you also must demonstrate that your work is making a valuable difference over time.

According to Heidrick and Struggles' Global Chief Information Security Officer Survey, 88 percent of CISOs present their results monthly to their full boards or to a cyber security board committee. This is a prime opportunity to communicate the results that you are delivering, as well as how your work supports the organization's mission and objectives.

As part of this, you will have to develop appropriate metrics and dashboards that you can share during those conversations. They need to convey your team's performance against any service level agreements you have in place, any risk measurement models or metrics you provide for your industry or area, and any further information that your board has requested. Most importantly, long-term trending data on your risk management performance compared to point-in-time data should be included that shows your current risk profile.

Getting the right mix of data that board members can drill into without going into too much detail is a fine line to tread. Too much detail and you can lose your audience or lead to unnecessary sidetracking. Too little, and the board can miss out on how much effort is taking place to keep the organization running efficiently and effectively. Most importantly, the metrics you bring to the fore should help your board understand what their decisions on risk mean in practice.

At one level, you should include measurements that show how your team has performed against SLAs. However, your SLAs normally exist for your benefit first, and while measurements like patching deployment in a given timeframe might help your team measure performance, they are not suitable for the board. Focus instead on specific critical issues mitigated in a given time frame. Just as you can use prioritization to improve your team's performance, this can ensure that your board knows where your efforts have been concentrated. It can also be a way to evaluate your current SLAs and whether they are still optimal. For example, taking 30 days to carry out patching in response to critical issues is not good enough today compared to the time needed to create malware or attempt weaponization around vulnerabilities.

Tracking critical risk mitigation times can show how well you focus, and how your team proactively deals with potential threats. At the same time, you can use this trend data over time to show how your organization is facing more or less pain points, and where your budgets may need to be adjusted to keep up. Compiling real-world data on your risk mitigation performance can also be used as part of any conversations that you have with your cyber insurance providers in order to reduce your premium costs by demonstrating a well-managed and maintained system over time.

This should also enable you to track your progression around performance improvements relating to security and risk management. At the start, you may find that you can make massive risk management improvements by adopting more best practices or by automating tasks like patch management and remediation. However, as you improve, the gains will be more marginal. This is actually a good sign that you have a mature and effective program in place, so manage expectations with your board over what this looks like. Setting expectations around risk

© Pipeline Publishing, L.L.C. All Rights Reserved.

management performance early will ensure that everyone knows what the end goals look like for IT security and provide you with the breathing room you need to pursue effective action.

The long-term goal around risk

Cyber security is one of those areas where one can never say that things are completed. There will always be more risks, more vulnerabilities discovered, and new threat actors trying to take advantage of misconfigurations in the cloud. For the board, this is actually a natural mindset to embrace that they should be familiar with from managing risks in other areas, whether these risks are due to potential supply chain and logistics issues, geo-political shifts, or wider economic trends.

The challenge for CISOs is how to support long-term organizational objectives and manage risk more efficiently and effectively over time. With so much of our business reliant on technology today, the role of IT security will take on more of that risk management ethos to keep things running whatever threat actors may throw at us.

Not for distribution or reproduction

© Pipeline Publishing, L.L.C. All Rights Reserved.