Diligent

Shifting Cybersecurity from Compliance to a Risk Focus

Table of Contents

Modern Organizations Now Realize That Cybersecurity Is a Crucial Concern

Cyberattacks have grown in frequency and sophistication, with 3,813 data breaches reported in the first half of 2019, which was an increase of 54% over the previous year.[1] And in light of COVID-19-related changes in workforce structure and an unplanned shift to remote work environments that might not be supported with the right infrastructure, companies became even more vulnerable to attack in 2020.

While enterprises know that cybersecurity protection is essential to safeguard their companies, many envision cybersecurity protocols as a compliance-focused approach to address industry and governmental regulations, rather than looking at them from a risk analysis level. This white paper showcases the key reasons to shift to a risk-based focus, and the best practices for doing so.

3,813

data breaches were reported in the first half of 2019, which was an increase of 54% over the previous year.

Diligent

The Evolution of the Cyberthreat Landscape

Although businesses have been online in some form or another for the past three decades, in the early years of the internet, the stakes were much lower for cyberattacks. Attacks tended to be driven by notoriety, rather than by financial gain. For example, in 1988, the "Morris worm"[2] spread throughout cyberspace and slowed computers to the point of being unusable; Robert Morris, the worm's creator, said that he was trying to find out how big the internet actually was.

At that point, organizations rarely stored confidential data such as client files, financial data and IP online; today, millions of companies do. As a result, we're far more likely to see cyberattacks that have significant fallout for companies in terms of operational problems, liability, IP theft and brand damage. And with the rise of internet-integrated devices such as smart appliances and self-driving cars, cyberattacks can impact the physical infrastructure we rely on, as well as the IP we store in the cloud.

IBM's 2020 Cost of a Data Breach Report found that the average cost of a data breach today is $3.86 million, and that it typically takes 280 days to identify and contain a breach.[3]

Many industries have already taken measures to determine minimum regulatory compliance standards to protect businesses' and consumers' online data. However, smart organizations are going even further by implementing a risk-focused approach to monitoring and managing cybersecurity, generally under the purview of the chief information security officer (CISO).

The role of the CISO has grown in influence—today, the CISO may report to legal, the chief information officer, the chief risk officer or sometimes all of the above. That's because cybersecurity is interwoven with all of these departments; it can't be siloed off. It's essential for a CISO to gain visibility within the organization by gaining champions to advocate for initiatives across different departments—one of which should be making the shift to a risk-based approach to cybersecurity.

Next, we'll talk about what that looks like in practice.

The Value of Risk-Based Approaches to Cybersecurity and Risk Management

So, what does it mean to adopt a more risk-based approach to cybersecurity, rather than focusing on compliance?

In a compliance focus, you'll look at your policies, standards, contractual agreements, regulations and legal mandates through a specific lens to evaluate whether each meets compliance standards. For instance, consider whether you have a control requirement such as malware protection implemented across your organization. From there, you need to consider to what extent the control is in place: fully, partially or not at all?

This approach has several benefits: it's easy to follow and easy to understand, and you can use a checklist to see how well your organization is performing. This approach can be adopted across many departments, and it works well in a relatively static environment.

However, it's difficult to update for dynamic environments, including disciplines like cybersecurity. And your approach may be at risk of either over-engineering controls, which can bring excessive costs when mitigating against risk—or under-engineering controls, which can lead to underinvestment and increased risk exposure.

Diligent

By using a risk analysis approach instead, you can use a formula for building your program that focuses on:

- Your risk profile: How susceptible is your company to risks, and what are those risks?
- Your risk appetite: What level of risk is acceptable, and how much are you willing to invest to mitigate it to that point?
- Your compliance obligations: What industry regulations do you need to put in place?

By focusing on risk management in cybersecurity, you'll gain access to more informed and actionable data, and greater transparency. This approach will provide you with an objective view of where your investment in cybersecurity should go. You'll gain an understanding of your cyber risk factors and levels of impact, and what mitigating actions you need to consider.

At each point, you can look at your risk appetite to understand whether you want to accept the risk, mitigate it or reduce the risk to an acceptable level. To understand the ROI of your risk mitigation initiatives, divide the financial return by the investment made.

When developing your risk management process, it's also important to accurately prioritize your risks—be pragmatic, based on what you know is achievable for your organization in a reasonable time frame. Conduct triage to understand the most costly or high-impact potential risks, and then focus on those mitigation strategies as a priority.

Once you've determined all of your risks, review your options. Will you accept the risk, which will lower the cost but increase the associated damage? Or will you mitigate the risk, which will increase your investment level but reduce your risk exposure?

Collaborate across departments to determine your response. Consider various factors, including costs, complexity, time scale to implement, disruption from change, business obstacles, training, end-user experience, testing and assurance. By documenting each risk and building a strategy for responding to each one, your organization will be far more prepared for potential cybersecurity breaches and other business risks.

What Does "Good" Look Like for Cyber Risk Management?

When building your risk management approach, keep best practices in mind. Here are some recommendations to consider:

- **Implement a steering committee.** Build a cross-disciplinary steering committee to help you report your risks across the organization, collaborating to determine which risks are the highest priority to address.
- **Balance your goals between aspirational and achievable.** As you put plans in place, make sure that you're focusing on objectives that aren't so pie-in-the-sky that they'll never be accomplished. A good rule of thumb is to consider only plans that could be implemented within the space of two years.
- **Grant your organization a grace period.** New policies and technologies can't be implemented instantly; keep a grace period in mind to give your organization time to research options and ensure a focus on implementation and education.
- **Focus on mission-critical systems and data assets.** Conduct triage, using an impact assessment to assess the criticality of each impacted system or asset from a business standpoint when determining what risks to prioritize.
- **Evaluate governance, risk and compliance (GRC) products to help streamline the process.** By choosing the right technology stack for your GRC initiatives, you can semi-automate the cyber risk process to minimize staff utilization.
- **Present the business argument to help establish a cyber risk approach.** Share a clear and dedicated plan with your stakeholders to improve your business's cybersecurity posture, including target investment, quick wins and best practices.
- **Establish a phased approach.** Don't attempt to "boil the ocean" by doing everything at once. Start with high-priority initiatives and grow your program from there.

Diligent

- **Extrapolate the risk insights to other areas of your security program.** Once your risk management program is in place, showcase the messaging through policy updates and a company-wide awareness and education program.
- **Promote the approach to your clients and partners.** By showcasing your strategic approach to cybersecurity, you can help improve your company's competitive positioning.

In the business risk assessment process, take these steps:

1. **Create a profile:** Start by setting up your business profile with an inventory of risks.
2. **Determine business impact:** What financial or reputational impact would each risk have on your business?
3. **Assess threats:** How likely is each threat to occur, based on historical data and industry data?
4. **Assess vulnerabilities:** What weak points currently exist in your organization?
5. **Determine risk:** Assess which risks are the highest priority.
6. **Treat the risk:** Based on the cost and potential impact, should you mitigate, avoid, transfer or accept each risk?

Keep in mind that cyber risk shouldn't be silo-based. Other departments will often need training and education around addressing cybersecurity concerns. For example, your HR department should implement policies around avoiding insider attacks, your awareness and corporate education team should develop a seminar on preventing social engineering attacks, and your supplier agreements should include appropriate language and minimum standards to lessen the risk of a third-party breach.

By ensuring you've built a comprehensive program that aligns with cybersecurity risk analysis best practices, you can generate buy-in throughout the organization and raise awareness of the importance of the work your team is doing.

The Importance of Automation for Cyber Risk Management

A robust cyber risk management process relies on automation and data analytics tools to ensure that your team is aware of the status of existing risks at all times, and that you'll be able to implement mitigation strategies immediately if a trigger action takes place.

Your risk monitoring technology stack should include the ability to set your risk appetite for each risk, monitor the risks, view risks in aggregate and report on the risk level for clear visibility throughout the organization.

- Be underpinned by industry best practices
- Utilize real-time data feeds to analyze new threats
- Anonymously share key information around incidents and threats
- Be intuitive to users without specialized industry training
- Provide industry-related data for risk assessments
- Provide investment versus impact figures for tracking ROI
- Offer flexible reporting options

Your solution should connect to disparate data sources for real-time threat analysis and vulnerability tracking. It should also integrate with your risk and regulatory frameworks so you can easily track risk appetite and verify compliance. By automating monitoring for changing risk levels or regulations, you can remove the operational burden of manual oversight. Your cyber risk analysts should receive automated alerts in situations where further action is necessary, reserving their time for issues that require strategic analysis.

By moving to an automated risk assessment platform, you'll be able to streamline your cyber risk management strategy, and have clear visibility at all times into your highest risks and any outside factors that may create potential vulnerabilities. That will enable your team to prioritize mitigating risks and fixing vulnerabilities quickly, rather than waiting months to discover breaches that have already occurred.

Diligent

Conclusion

As we've seen with the sudden shifts in work culture brought about by COVID-19, it's important to be aware of your potential risks and vulnerabilities. This will let you prioritize monitoring and mitigating when the unexpected occurs, rather than scrambling to build a plan on the spot.

By building a cybersecurity program that's focused on risk management, rather than on simply addressing compliance issues, your organization will have a heightened awareness, allowing a quick and predictable response to threats that arise and the ability to patch vulnerabilities as soon as they occur. A data-driven, automated threat detection and risk analysis process will provide the insights that your organization needs to maintain a safe and secure work environment in any scenario, even in light of a black swan event like the COVID-19 pandemic.

70%

of US-based CISO respondents to an Optiv Security survey said that company leadership had encouraged them to prioritize cybersecurity over all other business initiatives.

By proactively working to identify, monitor, manage and mitigate your risks as an organization, you'll be able to reduce the risk of major breaches that could seriously impact your company's operations, financial performance, and reputation.

Best-in-class companies know that investing in a robust plan to protect cybersecurity and monitor risks will pay performance dividends. In fact, 70% of US-based CISO respondents to an Optiv Security survey said that company leadership had encouraged them to prioritize cybersecurity over all other business initiatives.[4] Cybersecurity encompasses all business units, and a breach can have a huge negative impact throughout the organization.

By building an actionable plan and investing in automated technology to monitor and manage your organization's cyber risk, you'll gain an advantage over competitors who focus on compliance initiatives alone, and you'll have the data and analysis to help you choose the best and most cost-effective strategies to mitigate any issue that may arise.

Resources:

[1] https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report
[2] NATO, 2013, The history of cyber attacks – a timeline.
[3] https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542
[4] https://www.optiv.com/sites/default/files/2019-09/Brand_CISO-ResearchStudy_Report_091719.pdf

About Diligent

Diligent created the modern governance movement. As the leading governance, risk and compliance (GRC) SaaS company, we serve 1 million users from over 25,000 customers around the globe. Our innovative platform gives leaders a connected view of governance, risk, compliance and ESG across their organization. Our world-changing idea is to empower leaders with the technology, insights and connections they need to drive greater impact and accountability – to lead with purpose.

For more information or to request a demo, contact us today:
Email: info@diligent.com | Call: +1 877 434 5443 | Visit: diligent.com