WHITEPAPER

How to get C-Suite buy-in for cybersecurity solutions

By Rob Palermo, VP of Product Marketing
Kylie Ruiz, Sr. Marketing Manager

imprivata®

The way we work is changing, with enterprises across industries becoming more dispersed. The adoption of cloud-enabled business solutions and the necessity of third-party relationships and remote access have transformed industries. However, robust security strategies across industries lag behind the adoption of these new technologies. As a result, cyberattacks are on the rise. In the past 12 months, 54 percent of organizations have experienced a cyberattack; and 49 percent have experienced a third-party breach, up 5 percent year-over-year.

According to the IBM Cost of a Data Breach Report, the average cost of a data breach is now $4.35 million — and that number increases by $370,000 when a breach is triggered by a third-party. In fact, third-party remote access is one of the most dangerous — and expensive — attack vectors for any organization.

Even with the high costs associated with cyberattacks — especially as they relate to third-party remote access — it can be difficult to convince key decision makers and board members to invest in cybersecurity solutions. In this case, strategy matters — it's helpful to develop an executional roadmap for the often-complex decision-making processes that factor into cybersecurity procedures. Indeed, it's the opposite of making tactical or reactive recommendations based on a single incident or report. For example, pitching more robust cybersecurity solutions as broad "cyber risk mitigation strategies" — which hone in on malicious actors as well as vulnerable third-party access points and internal user error — could outweigh tactics that focus solely on stopping the so-called "bad guys."

Understanding and assessing risk resonates in the boardroom — doing so is a linchpin of any successful enterprise. Looking at cybersecurity solutions through a lens of risk management will ensure your recommendations are more compelling to decision makers and board members. Assessing risk is on every C-Suite agenda, after all.

ALL ABOUT ROI: THE FINANCIAL BENEFITS OUTWEIGH THE FINANCIAL RISKS

As we mentioned before, about half of all breaches involve a third party, so investing in vendor privileged remote access for third parties and vendors is critical for any organization with third-party relationships. More than half of organizations report experiencing a third-party data breach, with 70 percent of those organizations saying the breaches were due to too much privileged access.

Preventing this sort of breach will save in lost revenue, reputational damage (which is harder to quantify, but could cause the most damage in the long term), legal fees, ransom payments, regulatory fines, and other costs like system downtime.

Somewhat astonishingly,

50% percent of organizations don't currently monitor third-party access,

36% percent of organizations document the level of access granted for both internal and external users.

Of course, third-party breaches aren't the only threats facing organizations. Internal user error can also be catastrophically expensive and damaging, even if inadvertent. For example, say an employee for a pharmaceutical company accidentally impacts the manufacturing process for a given drug. This kind of mistake — most likely caused by inappropriate access — could set a company back months and cost it enormous sums of money in lost revenue.

We can also look to hospital settings, where thousands of employees might have access to electronic medical record (EMR) systems. Those internal employees are frequently the largest risk to an organization like a hospital because the data housed inside those systems is highly regulated and protected. Inappropriate access can result in noncompliance, regulatory penalties, reputational damage, and customer attrition. Although not an external cybersecurity threat, implementing stricter access controls and monitoring for this type of access is a critical cyber mitigation tactic that extends beyond malicious actors.

Most data breaches involve a privileged credential. Privileged access management (PAM) solutions can mitigate these risks, and there are several cost effective and low overhead solutions available on the market. Along with multi-factor authentication (MFA), PAM is a no-brainer for any organization interested in saving millions of dollars due to a breach that results in lost revenue, decreased productivity, reputational damage, or regulatory compliance issues.

Access solutions like PAM and vendor privileged access management (VPAM) also drive efficiencies for IT and security teams. This is crucial for enterprises across industries given the ongoing labor shortage in both fields. Most organizations set up accounts and access — both in-house and third-party — manually. These privileged access solutions automate these processes, freeing up IT and security resources, and cut down on the time it takes to investigate and remediate breaches or incidents if they still occur. These day-to-day savings add up quickly, and are easy to quantify when attempting to justify a solution purchase.

Organizations should also consider the importance of interoperability when updating and/or implementing cybersecurity and risk mitigation solutions. Where possible, it's smart to consolidate investments with strategic vendors who can help create a roadmap — and invest in making their solutions work together seamlessly. Otherwise, you'll wind up with siloed systems that don't provide teams with comprehensive visibility and control — adding frustration and inefficiencies on top of unmitigated cybersecurity risks.

Simply put, investing in cybersecurity solutions and risk mitigation strategies will more likely than not save an enterprise more money than it will cost it over the long run. When a cyberattack occurs, it's always more of a bleed out than a papercut.

BUILDING A BUSINESS CASE FOR CYBERSECURITY SOLUTIONS

Before pitching cybersecurity and risk mitigation solutions to the C-Suite, you should build out an airtight business case. For starters, it's important to investigate your current state and costs. Where are you currently spending your time and money? How many employees and third-party identities are you managing? How many more digital identities do you anticipate adding int he next year?

According to "The State of Cybersecurity and Third-Party Remote Access Risk," 48 percent of respondents don't have comprehensive inventories of their third parties due to the complexity in third-party relationships. That's a lot of unmitigated risk and a great case for any enterprise to integrate robust cybersecurity solutions.

Other key issues to consider when building out a business case include:

- Time spent on onboarding and offboarding user accounts
- Time spent, per month, managing and supporting access
- Time spent by IT department watching vendor and/or privileged activity in a session
- Money spent per year on additional/multiple license costs
- Number of downtime instances per year, and how long each lasts, on average
- Average cost per hour of downtime (including loss of staff productivity, incurred expenses, and lost revenue)
- Number of security and/or compliance incidents per year, plus time spent investigating
- Time spent creating reports and documentation for audits
- Amount spent per year on fines and/or penalties
- Current cybersecurity insurance premiums
- Access levels of internal users to determine in-house risks

Knowing all the above will help you accurately calculate inefficiency and downtime costs and anticipated savings, which will in turn give you a clear picture of anticipated return on investment. Again, the financial benefits of implementing strong cybersecurity and risk mitigation solutions will always outweigh the risks of not doing so, but to get C-Suite buy-in, it helps to show your work.

WHAT ABOUT THE CURRENT ECONOMIC CLIMATE?

As inflation rises across the globe and capital becomes increasingly difficult to access, organizations are, justifiably, operating with extreme caution. Every new investment is picked over with a fine-tooth comb. At every organization, the CFO is increasingly involved in every technology decision — something that wasn't the case even a year ago. But because cyberattacks are so common — and on the rise — cybersecurity and risk mitigation solutions are still broadly being approved by the C-Suite.

Business leaders understand now better than ever that a data breach, compounded with a potential economic downturn, could spell catastrophe for an enterprise. Investing in robust cybersecurity and risk mitigation solutions like PAM and VPAM is essential to the long-term health of any organization. As such, we recommend developing a credible ROI model (as addressed up top) for cyber investments to gain C-Suite buy-in and approval. Investing in a solution that simultaneously mitigates risks, makes users more productive, and saves the company money will not only be approved, but will build positive momentum for your cyber strategy and roadmap.

At the end of the day, cybersecurity threats aren't going away. (Indeed, they're becoming more frequent.) It's clear that both third-party access and internal user error present significant risks for organizations. But with robust access management solutions like PAM, VPAM, and MFA, organizations can protect themselves from the worst outcomes — namely, theft of sensitive data, reputational damage and significant financial losses.

We are happy to help you frame the discussion of investing in third-party identity and access management tools with your c-suite. Request a demo now!

REQUEST A DEMO

imprivata®

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For more information, please contact us at +44 (0) 208 744 6500
or visit us online at www.imprivata.co.uk.