WHITE PAPER

Thrive Through Transformation

> Gartner clients are also reporting that after years of quarterly reporting on cybersecurity to their boards, that boards are now pushing back and asking for improved data and understanding of what they have achieved after years of such heavy investment…"
>
> -Gartner, Inc., The Urgency to Treat Cybersecurity as a Business Decision, Paul Proctor, February 2020

INTRODUCTION

It's easy to forget that cybersecurity teams were facing significant headwinds going into 2020. After years of ever expanding budgets, new tech and new tools, a string of public breaches (in spite of the growing spend), hard questions from the board, and outcomes that were difficult to measure all raised significant questions for security and risk leaders as well as the industry in general.

Here's just a few of the issues that security leaders were facing going into early 2020:

- **Difficulty communicating cyber risk** to senior executives and board members
  - 72% of board members say they are more involved with security over the last 12 months[1]
  - 91% of board members can't interpret their organization's security reports1
- Challenges in **measuring program effectiveness and risk reduction**
  - 40% of security leaders default to using "worst case scenarios" to make a budget case vs. 43% using ROI[2]
- Dealing with **budget decreases**
  - In 2020 security spend has declined to 2015 levels after peaking in 2017[3]

….and then COVID-19 hit.

Since the pandemic started, there has been a significant shift in the security function as business itself has undergone radical and unprecedented changes. As many businesses continue to fight for survival, security teams are now focused on helping the business succeed in extraordinary times -- including enabling the massive shift of "work from home" employees, and rapidly onboarding technology to facilitate remote work and new business processes. Security teams have been forced to react quickly and adapt, and must still justify programs and spend to executive teams looking for any room in the budget to reduce costs.

Security leaders are under enormous pressure to do things faster, cheaper and deliver results, stressing programs that have relied on traditional or one-size-fits all "best practice" methods for managing their security.

Sources: A2018 BDO Cyber Governance Survey; Nasdaq: The Accountability Gap: Cybersecurity and Building a Culture of Responsibility

Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

Source: Gartner 2019

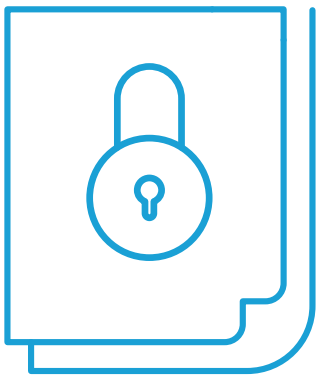
THRIVING THROUGH TRANSFORMATION

There are really two ways to look at the situation. Either the situation presented by COVID-19 is an existential threat to operations that will stress staff, systems and processes to the breaking point. Or, this is an opportunity to adapt your program to meet not only the challenges presented by the pandemic, but the pre-existing ones as well.

If you stop to think about it, it's shocking how many things are done a certain way in security because they have always been done that way. Conventional thinking, institutionalized ideas of "best practices," and the constraints imposed by the limits of technologies mean that most security programs look very similar, with similar results. And that's reflected in the overall state of security performance. As we noted in a blog post earlier this year, a quick look at the 2020 Verizon Data Breach Incident Report (or the 2019, 2018 and 2017 reports) show how little has really changed, and performance has stagnated across the board.

It's been clear for a while that rapid and fundamental changes are needed, but that level of reorganization can be almost impossible without disrupting operations-- which in ordinary times would present an unacceptable risk to the organization. But for better or worse, the disruption has already happened, and it's time to seize the moment and accept it as an opportunity to rethink your security program from the ground up to make it more effective, more agile, and better prepared for the security landscape of tomorrow.

This is a time of transformation, and an opportunity for security and business leaders to thrive by embracing it.



Learning the third-party's historical security performance through a calculated rating is another, more informative option for not only observing the company's reputation.

WHERE SHOULD YOU FOCUS?

This is a critical time to examine your security program and implement some key, and perhaps long overdue, changes. But with such a massive undertaking, where do you even start? Based on our work with thousands of organizations, we'd recommend starting with the following steps.

1. Measuring Program Effectiveness

How much are you spending, and what are the results you're delivering to the business? Focusing on results is critical here, but they have to be the right results. Too often security leaders focus on what was accomplished instead of the business impact, and often neglect to provide context for their reporting. For example, stating that 3 network penetrations were stopped this month isn't very helpful to a board member. Is that number good or bad? Is it more or less than last month? How does that compare to your competitors or the industry at large?

Instead, security leaders, executives and board members should focus on how security is aligning with the overall objectives of the business. For example, if one of the objectives is to reduce downtime in a SaaS product, security might report on the speed with which new cloud vendors are being onboarded and reassessed, as well as an increase or reduction in vulnerabilities found throughout the attack surface. Not only do these metrics correlate to business objectives, they get security leaders a seat at the table for higher level strategic discussions about how to execute a given strategy.

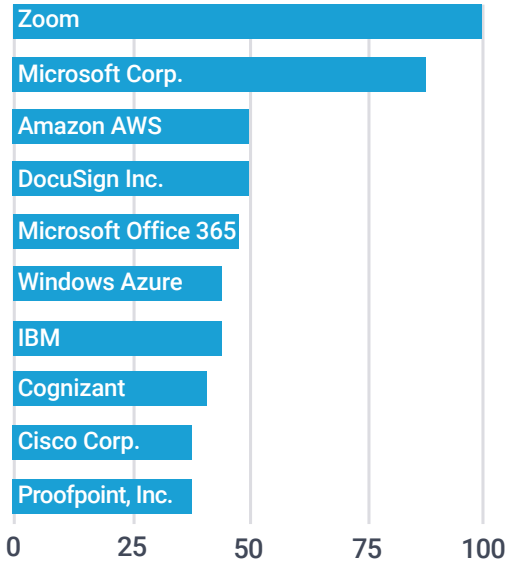
Benchmarking against other organizations within your industry or peer group is also a great way to demonstrate program effectiveness. Cybersecurity is increasingly becoming a key consideration when it comes to winning-- or losing-- business. In a recent study nearly 40% of respondents said they had lost business due to perceived lack of security rigor1, so knowing where you stand relative to the competition is powerful and actional knowledge that can be used to communicate to senior executives and boards the importance of your program. By showing relative performance, you can either demonstrate the efficacy of the program you've put in place, or argue for more resources to ensure the organization stays competitive.

2. Addressing The Expanding Attack Surface

The attack surface was already growing before the COVID-19 pandemic, but it has absolutely exploded since March 2020. With the large scale shift to work from home, any idea of a perimeter has disappeared, while the reliance on apps like Zoom, Microsoft Teams, Google Drive and Slack has seen new technologies both onboarded faster than ever and become more critical to operations than ever.

While security teams often did what needed to be done to adapt to changing circumstances, there needs to be a long term strategy for how to manage the ever expanding attack surface. In all likelihood, it may be years before the global workforce returns to the office full time-- if it ever does. So security teams need to prioritize getting visibility into their entire attack surface, including shadow IT and any corporate associated assets like old URL's or domains, understanding what their 4th, 5th and nth party risk is, and what their work from home risk exposure is. Afterall, you can't manage what you can't see, so it all starts with getting eyes on your security footprint.

Top Subscribed Companies Post-Offer



Top companies added to BitSight third-party portfolios since April 2020

Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

3. Focusing On Measurable Risk Reduction

For far too long the security field has looked at the world as a threat landscape. The problem with this approach is that security teams can end up buying technology and tools and without knowing exactly what they're trying to prevent, and then waiting for something bad to happen. While this approach may have worked in the past when the perimeter was the four walls of the corporate office, it is far from effective in the era of vast vendor ecosystems and far-ranging digital ecosystems where a more proactive approach is needed.

Instead of measuring how security controls are working, security leaders, executives and boards should focus on risk. When you switch to looking at the world as a risk landscape, you switch to a worldview that emphasizes visibility and probability. Business leaders need to understand that initiatives like digital transformation, or shifting the workforce to remote work will introduce risk into the system, and security leaders should focus on having visibility into which vendors, digital assets or work from home networks present the most risk to the organization. This will both help to generate actionable and proactive strategies and plans, and give security leaders, executives, and board members more meaningful KPI's to track to understand how the actions of the security team or the rest of the business are impacting the organizations cyber-risk profile.

72%

of board members are involved with cybersecurity now, but only 9% understand their organization's cybersecurity reports.

4. Optimizing Cost and Finding Efficiencies

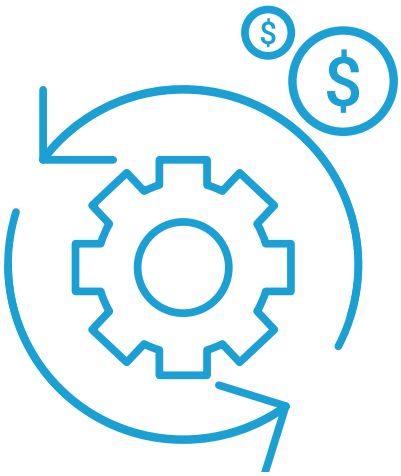
According to Gartner, cybersecurity budgets have been steadily decreasing for the past several years, from a peak average of 6.2% of total IT spend in 2017 to 5.7% in 2019, and the trend has only continued into 2020. While the overall movement isn't huge, it's trending in the wrong direction, and putting security leaders under pressure to optimize their programs.

One of the most effective ways to make your program more efficient is to increase the use of automation. This is most apparent when it comes to Third Party Risk Management programs.

TPRM programs can be one of the most time- and resource-consuming parts of your security program. Manual assessments take a long time to get back from vendors and process, the responses are often qualitative or impossible to verify, the information contained in them only captures a moment in time and is seldom actionable, and oftentimes an on-site visit may be required. It all adds up to a lot of personnel hours and expense dedicated to checking boxes with vendor security.

It's no wonder TPRM is one of the places where small changes can lead to massive operational efficiencies that can make your program faster, less costly and more scalable. Using automation to tailor vendor onboarding assessments and reassessments can save significant time and cost compared to traditional manual processes.

Automation can also make securing your work from home and cloud attack surfaces more manageable by helping you spot the gaps in your security visibility, and making asset inventories more complete. This cuts down on the hours required to build, maintain, and monitor asset inventories, or chasing down shadow IT.



5. Communication Is Key

As noted earlier, 72% of board members are involved with cybersecurity now, but only 9% understand their organization's cybersecurity reports. These two numbers illustrate that there is a two-way communication gap when it comes to security. As we discussed earlier, security leaders need to become more adept at the types of information that is communicated to the board and executives.

For Security Leaders:

CISO's must communicate with board members and leadership in the business terms they are used to dealing with. That means framing the performance of your security program in terms of outcomes, risk reduction and business impact.

Some issues to focus on in your reports:

1. Where is risk present in the digital or vendor ecosystem, what steps are being taken to reduce it, and what impact will that have on overall security performance or the likelihood of a security incident?
2. Has the company's ability to respond to a security incident improved?
3. How has security enabled the business overall? For example, has the average time to onboard a new vendor been reduced? Have costs been reduced? Has there been an impact on the use of shadow IT?
4. How does the company's security performance rank relative to competitors or the industry in general? Is there a strategy to improve or retain the advantage?

For Board members:

Board members and senior leaders also need to become better at providing direction to security leadership. Boards have a responsibility to investors, shareholders and customers to ensure cybersecurity is properly implemented. They can't just sit back and accept what is reported on. Boards have the right to ask questions and give direction and guidance to security leaders. But to do that, board members and executives need to become better informed about security strategy and how it fits into the overall business strategy.

Board members addressing cyber risk should be focused on a few key issues:

1. Has the board evaluated and approved the company's cybersecurity strategy?
    a. Boards should evaluate and approve a strategy affirming the company's commitment to minimizing the likelihood that a cyber incident would have a material impact on the business.
2. Is the company organized and resourced appropriately to address cybersecurity risks? Does management have the skill sets it needs?
3. How does the board evaluate the effectiveness of the company's cybersecurity efforts? What measurements and metrics are useful in evaluating performance?

90%

of security leaders believe or strongly believe their role in the business needs to be more strategic, but 60% feel that they primarily act as day to day managers.

(Source: IDG research (in collaboration with BitSight)

A TIME FOR PROFESSIONAL TRANSFORMATION

In addition to thriving through the transformation of your security program, this also an opportune time to think about professional transformation. Security leaders need to examine their professional journey as their programs become a driver of business growth and transformation, with a focus on communication and business skills.

In a 2019 joint study by BitSight and IDG, 90% of CISO's believe or strongly believe that their role needs to become more strategic, but 60% feel they act as day to day managers. The gap between where CISO's envision their role going, and where they currently are is striking. But focusing on the "business skills" outlined above-- measurement, management, reporting and communication, will help close that gap.

The biggest question security leaders need to be asking themselves is "how can I be a partner to the business?" The goal is to be seen as a trusted partner in growth, rather than a barricade or an obstacle that will slow projects down or delay growth initiatives. Reaching out to build relationships with other leaders in the business, understanding their objectives, goals, challenges and pain points, and working collaboratively to create plans and strategies will pay dividends down the line and earn CISO's a seat at the table where they are able to influence initiatives at the outset instead of reacting once plans are already in motion.

Developing the ability to communicate security's work in terms of business outcomes, or ROI, will also be of benefit down the road when it comes time to ask for more budget, tools, or headcount. Instead of merely asking for more money to respond to a threat or implement new tools, proving how security has contributed to growth and enabled the business, and demonstrating where investments need to be made to reduce risk and improve operational efficiency may be a more effective approach in the boardroom and establish the CISO as a trusted advisor and partner to the business.

4 KEY TAKEAWAYS

1. **Measure the effectiveness of your program and report to senior executives and boards**

   Measure your program in terms of business outcomes and how you're enabling the business to meet its goals is key. Whether it's benchmarking against the competition to show how security performance management is enabling the company to win new business or keep existing clients, or demonstrating how efficiencies in the TPRM program are allowing the business to stay agile through a fast and scalable onboarding and reassessment process, there are plenty of KPI's that boards are looking for to ensure the program is generating positive ROI.

2. **Focus On Risk Reduction**

   Instead of focusing on threats and how you're reacting to them, focus on risk and how you're reducing it. We'll never live in a world with perfect security, but setting expectations and demonstrating how your program is reducing risk can demonstrate that the security team is taking a proactive and measurable approach to keeping the organization.

3. **Gain expanded view into the increasing attack surface and work from home environment**

   The attack surface has expanded dramatically since the first quarter of 2020 and shows little signs of shrinking. It's more vital than ever that security leaders get visibility into their work from home footprint, cloud assets and accurate assessments/reassessments of their third party vendors.

4. **Reduce costs through automation of processes**

   Security teams were already facing declining budgets, and with changes to traditional operating processes, there is more pressure than ever to be more efficient. Increasing the use of automation, especially in time- and resource-consuming TPRM programs can create huge operational efficiencies that enable the business to be more agile in its strategy by onboarding vendors faster, with less cost, and at greater scale.

Want to learn how Security Ratings can help your organization Thrive Through Transformation?

Get a demo today and see how

Visit www.BitSight.com for more information

BITSIGHT®
The Standard in SECURITY RATINGS

111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of data on security issues. Seven of the top 10 largest cyber insurers, 20 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit **www.BitSight.com**, read our blog or follow **@BitSight** on Twitter.