
4 KEYS TO
PROVE SECURITY
IS NOT A
COST CENTER
Balbix®

Why Security is Perceived as a Cost Center

Cybersecurity is expensive. There's no getting around it. Protecting the rapidly expanding enterprise attack surface requires significant investments in talent and enterprise-grade products. Both come at a high cost.

In the midst of rising threats, it is common for stakeholders to grant sizable funding for cybersecurity in reaction to a breach or to quell rising fears of a breach. When these threats become less immediate and worries subside, the benefits associated with cybersecurity costs can be forgotten. How then, do cybersecurity leaders avoid this troubling cycle of knee jerk investments and help stakeholders see the value of their security program, even when things feel secure?

This starts with being proactive about breach avoidance and taking a risk-based approach to cybersecurity planning and strategy. Every organization has unique weaknesses and areas of infrastructure that are more business-critical than others. A CISO's strategy should revolve around these unique risk areas, deploying teams and tools to defend the most important areas of the business based on what is currently fashionable for the adversary.

In this guide, we'll cover how to proactively manage your cybersecurity program and prove that it is not a cost center by:

1

Using powerful metrics

The key to a proactive approach that will be backed by stakeholders is understandable metrics. Being able to quantify breach risk and explain the issues driving risk with metrics is vital to helping board members appreciate the value of investments.

2

Speaking the board's language

Metrics don't have any utility if stakeholders don't understand them. The board only really wants to know 3 things about cybersecurity and a conversation that focuses on answering these questions is important to getting their buy-in.

3

Leveraging cross-department collaboration

Getting cybersecurity buy-in across the company is essential. Effectively communicating the importance of security programs, building relationships with other business units, and aligning with the company mission are all important to executing initiatives that require employee participation.

4

Getting accurate, explainable assessments

The accuracy and explainability of your security posture assessments are the foundation for proving security is not a cost center. There are several billion-time varying signals in the enterprise and you need a system by which to capture and make sense of it all.

Using powerful metrics

In order to prove something, you need hard evidence. The best form of hard evidence is numbers. The problem is that in cybersecurity, there are thousands of important metrics. So which ones should you use?

There are two main things you should consider when choosing which metrics you'll cite for getting or maintaining stakeholder buy-in for your programs:

1. What are our greatest weaknesses or areas of risk?
2. What metrics are tied to our current investments?

If your greatest area of risk is phishing, like 89% of the respondents in our 2020 Security Posture Report, your key metrics might be:

# of repeat offenders for phishing incidents

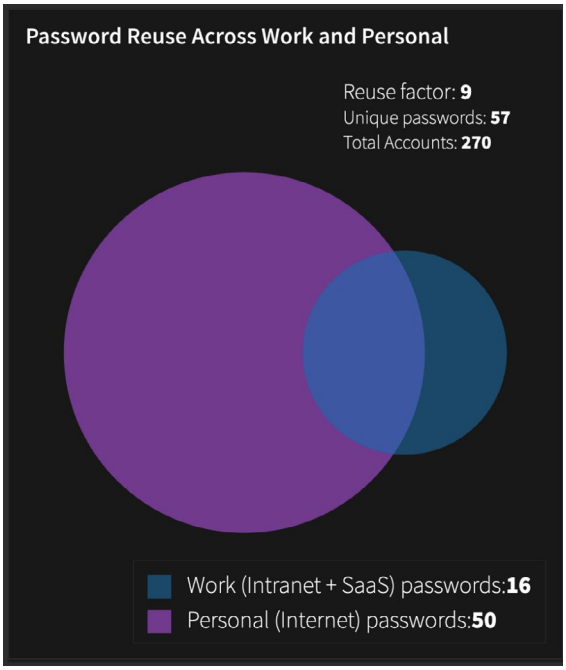
# of phishing-like emails delivered to employee inboxes

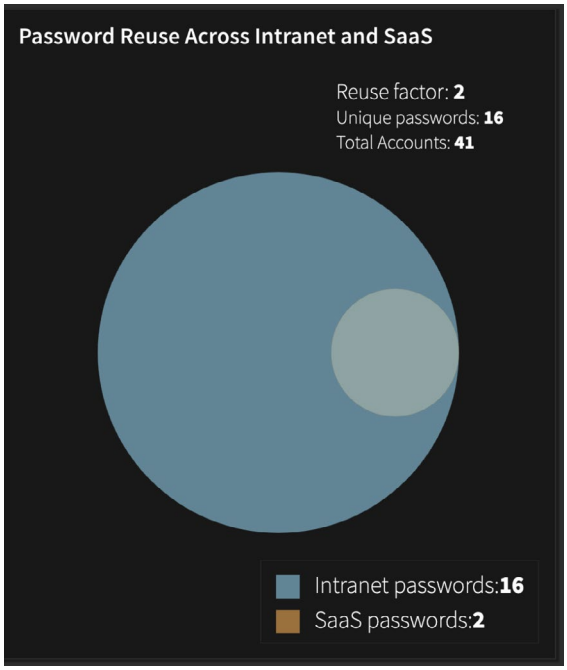
An important focus for any security team is the password hygiene of users, especially those that are privileged. Improving password hygiene typically requires investment in a password manager, two-factor authentication software, and training. Metrics that can be used to show the importance of these investments could be:

# of reused passwords among work and between work and personal accounts

# of weak passwords among privileged users

# of passwords being stored or sent in the clear every week





Cyber risk Reporting metrics

Below is a full list of metrics that can be used, based on the categories of risk that you want to highlight.

Overall risk

METRICS	SAMPLE VALUE
% likelihood of a breach. Calculation = f(vulnerabilities, threats, exposures, mitigating controls)	45%
$ impact of a breach	$ 1,000,000
$ risk score of a breach. Calculation = Breach likelihood x impact	$ 450,000
$ security incident costs to date	$ 250,000

Unpatched software

METRICS
# of assets with critical CVEs
# of assets with CVEs mentioned on the dark web
% of systems that are unpatched
# of software vulnerabilities detected, broken out by low, medium, and high likelihood of breach
Average time to patch by criticality level
# of vulnerabilities patched in last month, quarter, etc.
# of critical assets patched in last month, quarter, etc.
% of critical vulnerabilities remediated

Weak and compromised credentials

METRICS
# of weak passwords (on privileged user assets)
# of reused passwords (on privileged user assets)
# of passwords shared across work and personal (among priviliged users)
# of business critical assets with protocols using passwords in clear
List of insecure protocols transmitting clear passwords

Phishing, web, and ransomware

METRICS
# of users clicking on emails marked as phishing last month
# of users visiting unsecure and spam like websites
# of repeat phishing offenders

Certificates and encryption

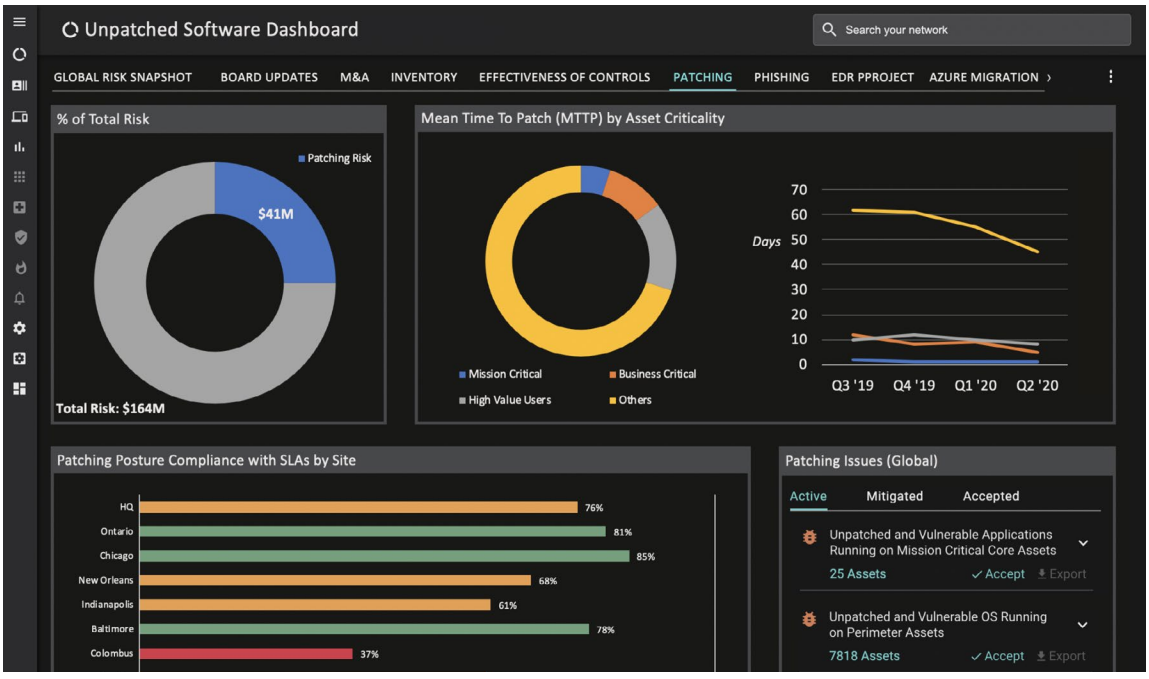
METRICS
# of expired certificates
# of self-signed certificates
# of users clicking through certificates
# of certificates with weak encryption protocols
# of assets with unencrypted administrative traffic
# of assets with unencrypted email/SaaS/messaging traffic

Trust relationships (propagation)

METRICS
# of server assets susceptible to exploitation of trust via admin protocols
# of networking assets susceptible to exploitation of trust via admin protocols
# of admins with high likelihood of breach
# of admins caching credentials

Security controls

METRICS
# of attacks blocked
% of pentest/red team actions detected
# of issues detected by endpoint security
# of repeated security incidents



Example of a customer dashboard with key patching metrics.

Speaking the board's language

The main question your board has is, "Are we secure?" As you know, that is an overly simplified and arguably unanswerable question.

No enterprise is 100% secure and, given enough adversarial effort, any organization can be breached. Instead of discussing cybersecurity as a binary objective, CISOs and CIOs can help their board members think of cyber risk as a spectrum.

When considering this spectrum, there are three questions that your board has in mind. Your job is to help them answer:

1. Where are we on the cyber-risk spectrum?
2. Where do we want to be?
3. How do we get there?

---

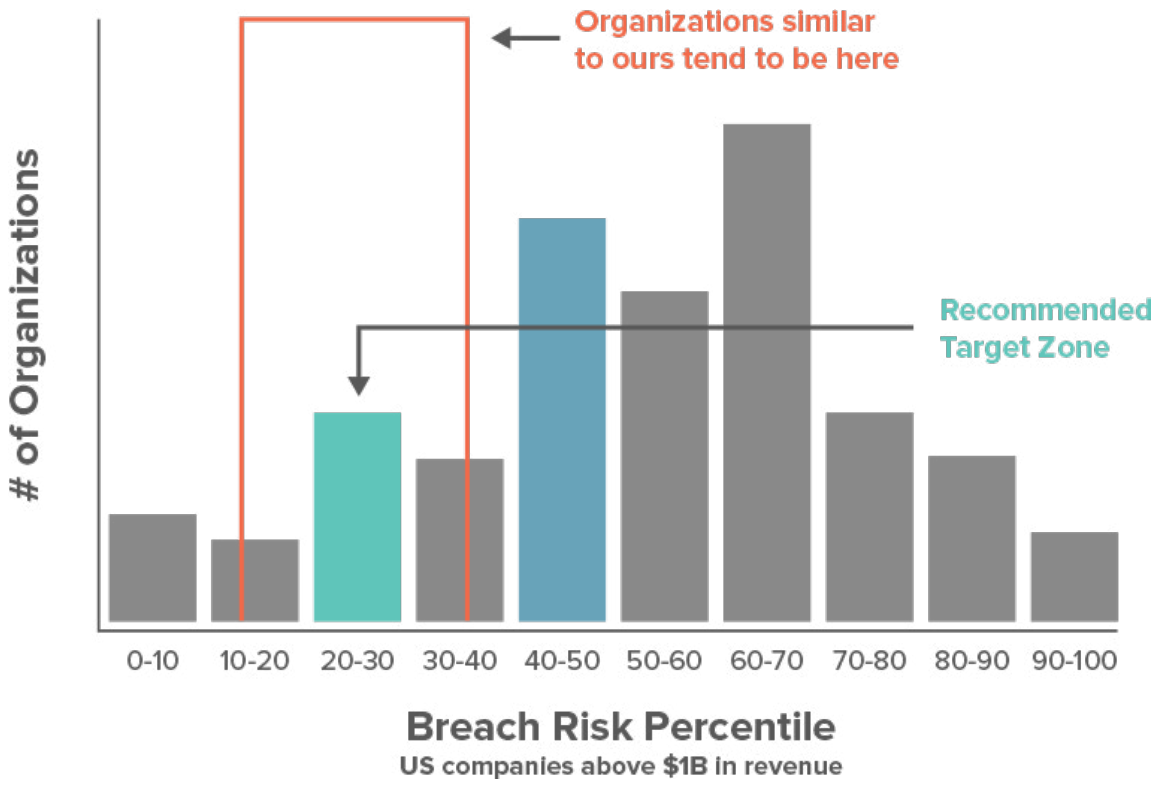
1. Where are we?

To get the conversation rolling, identify where your company is on the cyber risk spectrum. Quantify your views with risk scores based on your current security controls and the business impact of a breach. Benchmarking your cyber risk against similar organizations can also help to understand where you are.

Cybersecurity metrics are not tangible for non-technical stakeholders, so framing risk in terms of dollar impact to the business can be a good way to level the conversation. For more information on calculating and sharing your cyber risk levels, check out our eBook on Decoding Cyber Risk.

2. Where do we want to be?

An open conversation with the board and senior colleagues about where the organization should be on the cyber risk spectrum is key to getting alignment. If your company is like most, you're on the yellow part of the spectrum quickly slipping into orange and red. Your attack surface is rapidly expanding as data grows and technology accelerates. In addition, your employees are likely shifting towards remote work, which brings a whole new layer of security concerns.



Depending on the type of customer data you store or sensitivity of IP you own, being in the yellow/orange risk area may or may not be acceptable. Share your thoughts on where you think the organization should be given the potential impact of a breach in dollars. Institutions like Equifax, large banks, and the Pentagon should invest in cybersecurity to the point where chances of a breach are almost non-existent. Most other organizations will have a risk appetite that falls somewhere in between light green and orange on the spectrum.

3. How do we get there?

The board has come to a consensus on the appropriate cyber risk level for your organization given the available budget and the criticality of a potential breach. Now they want to know: how do we get there?

In order to answer this question effectively, CISOs need to know the most vulnerable areas of their security posture. Cybersecurity technologies like Balbix have this intel available in real-time, with risk heat maps and prioritized risk insights.

Present the top three to five risk groups that need to be addressed to decrease cyber risk, detailing the likelihood of a breach and business impact of a breach for each area. Then, give a plan of attack for mitigating each, whether it be a software update project, an investment in a new tool, a training for certain risk owners, or something else.

Example of customer dashboard used for board updates.

Everything comes to light during an incident

Software is fragile, people make mistakes, and despite robust investments, any organization can be breached. The true ROI of your security investments will be on display for everyone to see during and after an incident when you're able to contain the impact of a breach or lose control entirely. Investigating the incident after the fact will also bring to light whether the right investments and enough investments were made in cybersecurity.

Breaches happen in 4 stages, starting with the perimeter being compromised and ending with sensitive data being exfiltrated from an enterprise's systems. It can take months for these 4 stages to play out and the visibility you have into network traffic and abnormal behavior will determine at which stage the breach is detected. Visibility into how the breach played out is also vitally important. A transparent, and timely report of a data breach's extent will give stakeholders confidence in a CISO's ability to make data-driven investments moving forward.

The value of specific security measures will also become apparent during and after a breach. Controls that prevent misconfiguration, unencrypted communications, and strong user and device identity will play a large role in preventing attackers from accessing target systems.

Leveraging cross-department collaboration

Getting employees across the company on board with your cybersecurity mission is vital to executing on your plans and delivering on risk reduction goals. For the majority of audiences in your company, communicating your approach to cybersecurity with technical terms will go in one ear and out the other. Many departments, like the board, need more simplistic explanations for cybersecurity that center on risk to the organization and avoid language-related to IT, networking, software, and configurations.

Communicating the importance of cybersecurity

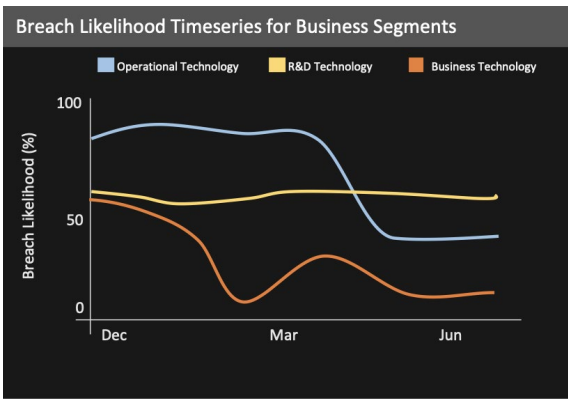
Many non-infosec employees don't give much thought to the importance of cybersecurity because its effects on them are not palpable and they don't feel that their role in security is significant. To help employees across the business understand the importance of cybersecurity, emphasize the financial impact of a breach to the organization. Then explain how breaches often start at the employee level with avoidable errors like password reuse, clicking on phishing emails, and out of date software. Last, emphasize the impact that getting compromised can have on someone, from their device not working properly to their personal information being sold on the dark web.

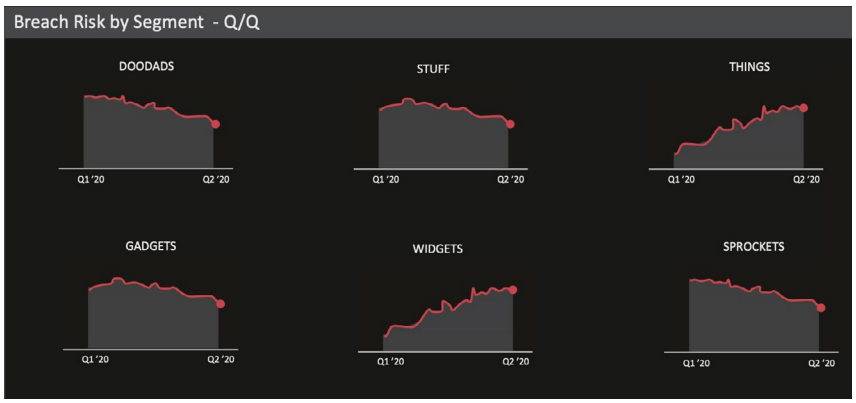
With this in mind, the time required to set up a password manager and update critical software in a timely manner should not seem like as much of a hassle to the average employee. No one wants to be the reason that their organization is breached. Moreover, no director wants their business unit to be the starting point for a breach.

Building relationships and furthering the mission

Communication is key, but even more consequential is the relationship infosec has with various departments. CISOs and other cybersecurity leaders should be actively engaged with other leaders in the organization, helping them be secure while minimizing the legwork necessary for good cyber hygiene. Mutual value exchanges are required for cross-department collaboration in every organization and infosec teams should identify the ways that they can bring value to the unique needs of other teams.

A good common point for cross-department collaboration is the company mission. Your organization likely has a focus in its mission statement on innovation, digital transformation, and technology. Tying initiatives back to the corporate mission minimizes friction and motivates other departments to do their part for a greater cause.





Examples of dashboard modules that customers use to track risk metrics by business segment.

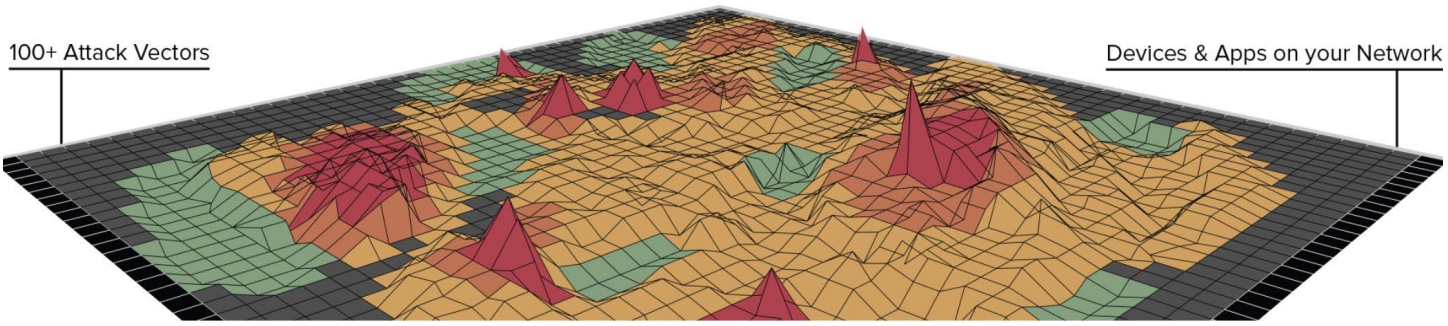
The challenge of accuracy and explainability in cybersecurity

Ultimately, proving that cybersecurity is not a cost center comes down to how well you can assess and report on breach risk. Ask yourself, can you do this in a way that:

- Aligns with the business?
- Is explainable and backed by data?
- Clearly highlights deficiencies and progress?

Although it may seem simple, for many cybersecurity leaders this is a pipe dream. For one, it's difficult to align your plan with business goals due to gaps between the business level view and the inherited IT/cybersecurity level view. There isn't a reporting framework that can generate different types of reports appropriate for various scenarios and audiences. The board and exec staff don't understand technical security concepts and frequently confuse compliance and security.

Understanding the business criticality of assets is a massive project in itself that can take months, if not years to complete. There are also many infosec teams that don't know how many IT assets they have. Mechanisms for IT asset inventory are not up to date (manual, not real-time/continuous) and incomplete (cloud, mobile, IoT). The incomplete inventory that does exist has no concept of measures important to risk calculations, such as business criticality.



Assessing and reporting breach risk with Balbix

Balbix's 3rd generation security posture platform provides a comprehensive view of your attack surface and the risk level for every asset across 100+ attack vectors. This 24×7 analysis covers on-prem, cloud, and mobile assets including unmanaged systems and non-traditional assets.

Prioritized risk insights take the hassle out of sifting through vulnerabilities and allow security teams to mitigate business-critical risks first. Drill-down heat maps make the process of reducing risk even easier and lend to cybersecurity presentations where risk across an enterprise can be more easily explained.

Quantifying breach risk for senior colleagues and the board becomes a breeze when you have simple risk scores for every business unit and asset groups, along with breach likelihood and impact metrics to support your proposed plans. Once you've embarked on the security posture transformation journey, you can use risk trend graphs to show how your investments are reducing risk across the enterprise and saving the business money.

Balbix®