Balbix®

ATTENTION CISOs:

# 5 Board Presentation Mistakes

TO AVOID AT ALL COSTS

**AS A CYBERSECURITY LEADER,** you generally receive only a short period of time in the board meeting for your update. During this time, you need to communicate key risks and remediation tactics, explain your strategic goals and plan, and answer questions; all with a largely non-technical audience. This can be quite challenging. Your presentation needs to be crisp, engaging, and informative, and you can't afford to make any mistakes.

## WHAT THE BOARD CARES ABOUT

1 Revenue growth and other non-revenue objectives related to the mission statement

2 Current and future expenses

3 Compliance, threats to future revenue and brand reputation

# 5 common errors IN BOARD REPORTING AND HOW TO AVOID THEM

## 1 Not speaking the board's language

The board's perspective of cybersecurity is different from that of the infosec function and IT teams. The board views security as a set of risk items that need to be accepted, managed, or mitigated depending on the expected impact to the business. Boards want to know the business impact of the security risks and investments.

How can I improve my presentation for next time?
Don't focus so much on the technical details.
Demonstrate the value of security investments through lower risk.
Show us an operational plan!

### TIPS

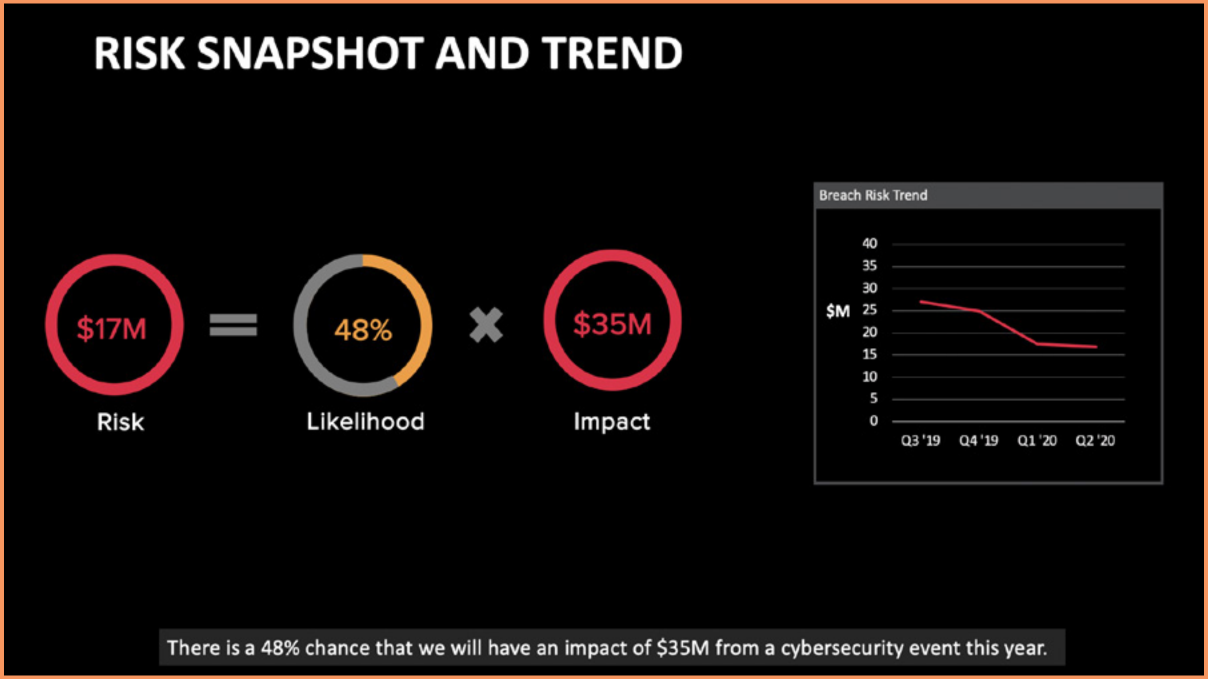
**You must develop a good understanding of your board members' risk appetite and your presentation must speak about risk in metrics relevant to the board, i.e., in money terms.**

**Instead of focusing on the technical details and costs of new technologies, demonstrate the value that the cybersecurity investment has brought to the organization through lower risk.**

# 2 Not presenting an accurate picture of your risk

With a massive and rapidly growing attack surface, the challenges of understanding and improving cybersecurity posture are immense.

> *"According to a recent Governance Outlook from the National Association of Corporate Directors (NACD), 82% of board members are secure in their management's ability to address known risks, but only 19% have the same confidence about atypical, disruptive risks."*



RISK SNAPSHOT AND TREND

There is a 48% chance that we will have an impact of $35M from a cybersecurity event this year.

The three essential prerequisites for getting a complete picture of your risk are:

- An accurate up-to-date inventory of assets to be protected
- An understanding of the business value of these assets
- Continuous analysis of these assets for cyber-risk across all relevant attack vectors

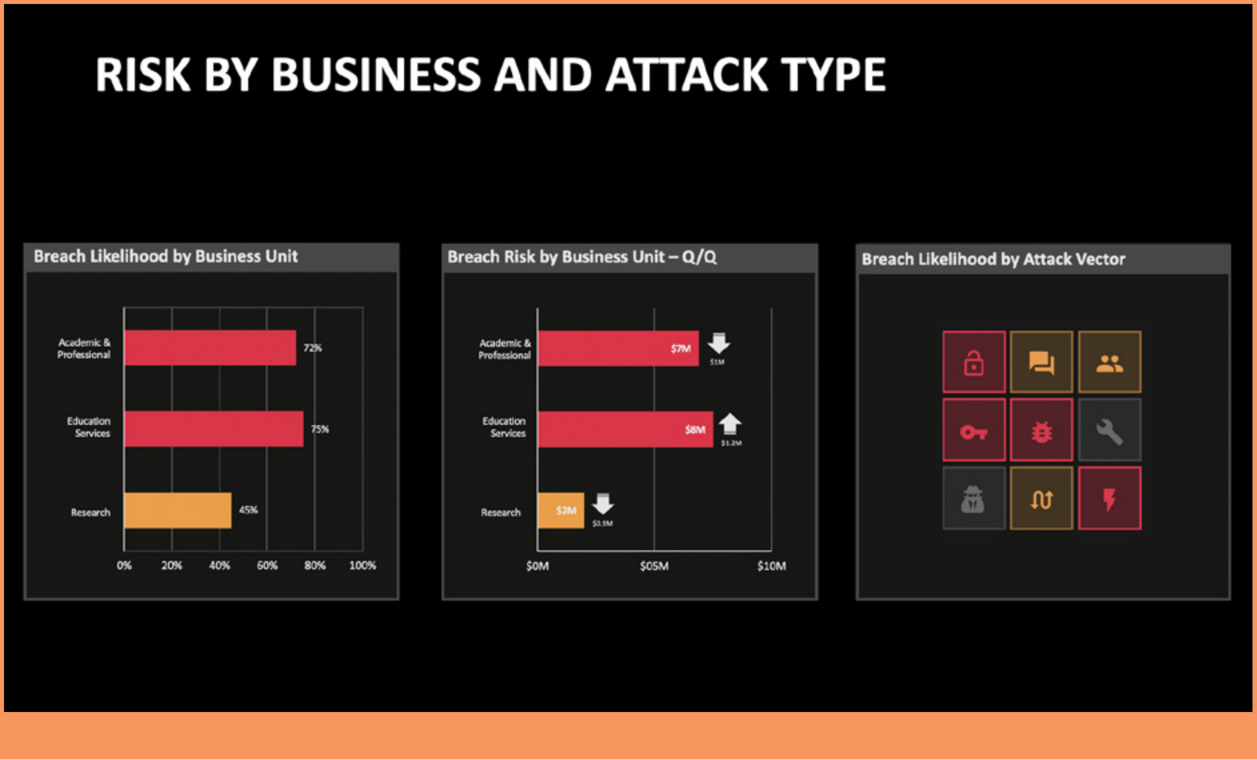
## TIPS

**Gain the trust of your board by acknowledging the reality of a challenging and enormous attack surface.**

**Once you have complete information about your asset inventory, you will be able to define risk areas appropriate for your business and then map your vulnerabilities to these areas.**

**For example, one such risk area can be "intellectual property." When you analyze, prioritize and remediate vulnerable assets that contain intellectual property, your reporting to the board will be based on actual, on-network ground truth.**

# 3 Not being able to quantify your security posture



RISK BY BUSINESS AND ATTACK TYPE

Breach Likelihood by Business Unit

Breach Risk by Business Unit – Q/Q

Breach Likelihood by Attack Vector

The board can sometimes view cybersecurity as a difficult technical topic. As a result, many board and C-Suite decisions related to security are made with gut feelings and with insufficient data.

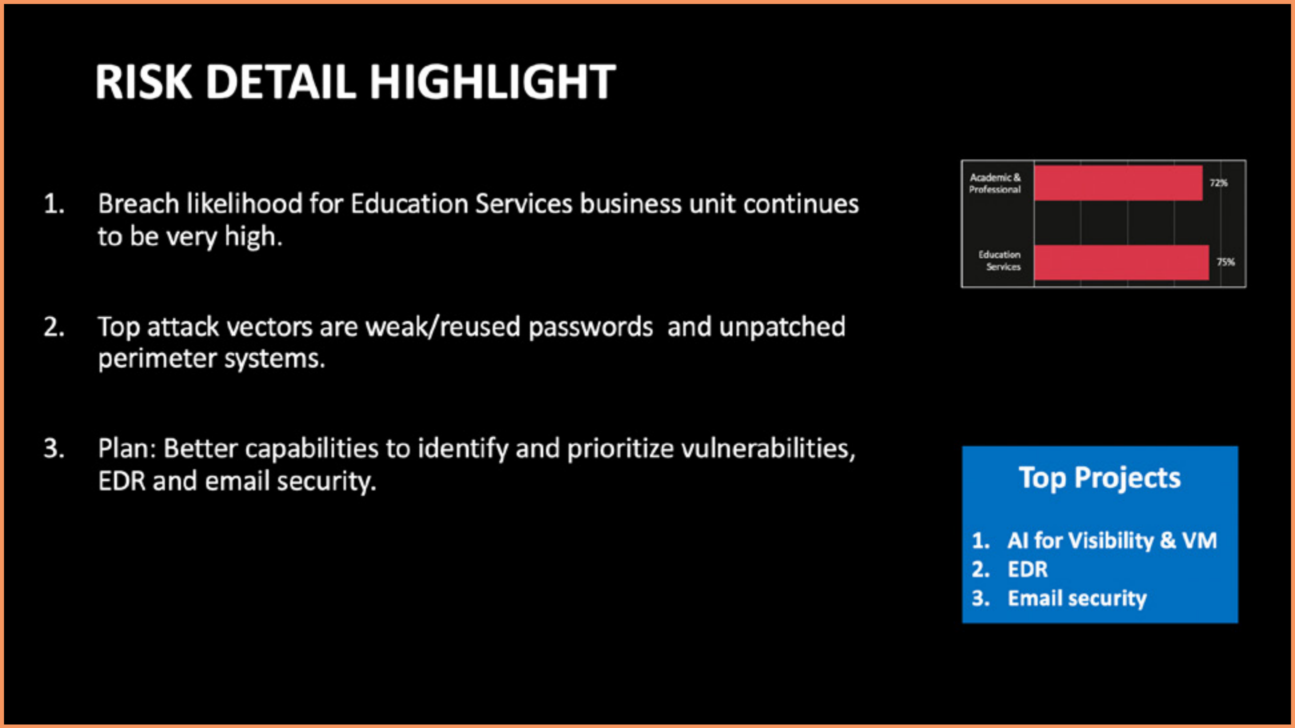
## TIPS

Overcome this obstacle by presenting risk in units of money. Board members may not understand what a "high risk score of 90" or a "target patching cadence of 22 days" means, but they certainly understand the implication of "$8M of risk due to unpatched software."

Once key areas of the business at risk have been identified, quantify the risk in money terms and help the board understand how your cybersecurity program is aligned to mitigating this risk.

# 4 Presenting too much information

You see the growing volume and increasing sophistication of cybersecurity attacks, so it’s not surprising that you seek to share detailed information with the board, while explaining the resources you need to counteract those threats. Boards want to make decisions informed by data, but beware of presenting too much. It might overshadow your main point.



## RISK DETAIL HIGHLIGHT

1. Breach likelihood for Education Services business unit continues to be very high.
2. Top attack vectors are weak/reused passwords  and unpatched perimeter systems.
3. Plan: Better capabilities to identify and prioritize vulnerabilities, EDR and email security.

Academic & Professional
72%
Education Services
75%

**Top Projects**

1. AI for Visibility & VM
2. EDR
3. Email security

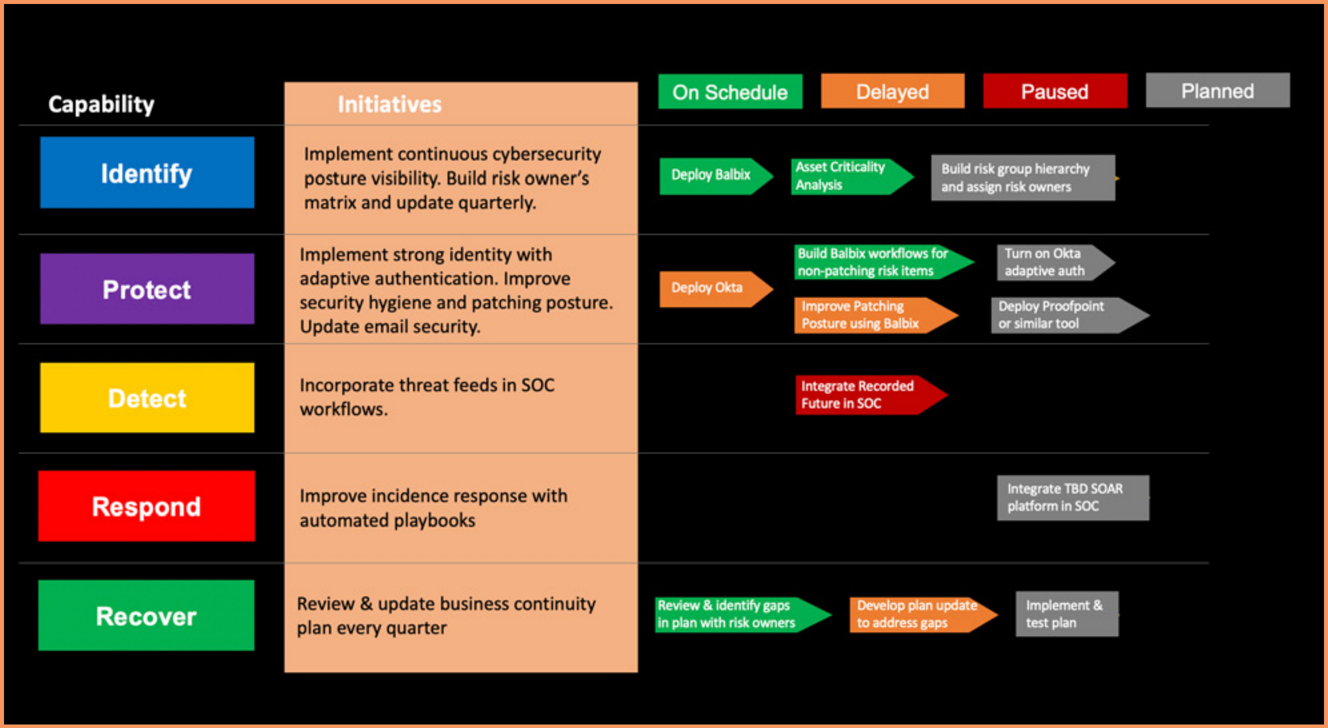
## TIPS

**Tell a compelling and simple story. Balance facts with insights. Instead of just reciting results or data, provide an analysis.**

**Explain why something happened, along with the ramifications. Tell them where you are and where you need to be from a cybersecurity posture perspective.**

**Share information about new risks and new opportunities to improve (building on what you presented in the prior meeting).**

# 5 Not having an operational plan



🟩 On Schedule 🟧 Delayed 🟥 Paused ⬜ Planned

| Capability | Initiatives | |
|---|---|---|
| Identify | Implement continuous cybersecurity posture visibility. Build risk owner's matrix and update quarterly. | 🟩 Deploy Balbix<br>🟩 Asset Criticality Analysis<br>⬜ Build risk group hierarchy and assign risk owners |
| Protect | Implement strong identity with adaptive authentication. Improve security hygiene and patching posture. Update email security. | 🟧 Deploy Okta<br>🟩 Build Balbix workflows for non-patching risk items<br>⬜ Turn on Okta adaptive auth<br>🟧 Improve Patching Posture using Balbix<br>⬜ Deploy Proofpoint or similar tool |
| Detect | Incorporate threat feeds in SOC workflows. | 🟥 Integrate Recorded Future in SOC |
| Respond | Improve incidence response with automated playbooks | ⬜ Integrate TBD SOAR platform in SOC |
| Recover | Review & update business continuity plan every quarter | 🟩 Review & identify gaps in plan with risk owners<br>🟧 Develop plan update to address gaps<br>⬜ Implement & test plan |

Your board presentation must be backed by a strategic plan detailing how your initiatives and programs will change the cybersecurity posture and achieve the appropriate level of residual risk.

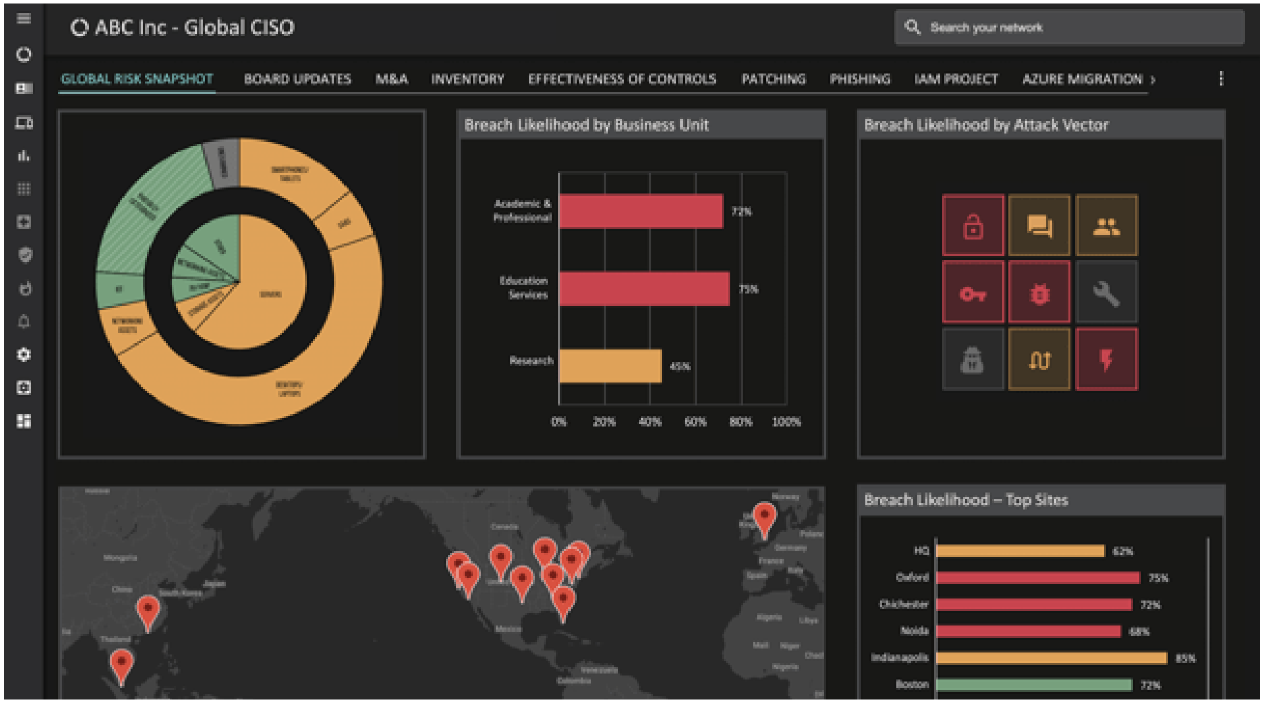
## TIPS

Present your plan as an easily digestible, high-level list of initiatives or projects, each with corresponding time frames, required resources and a dollar cost.

Qualify the responsible stakeholders involved and ensure that your board understands that the 1st line of defense for cyber-risks are the risk owners in IT and in the business, and not the infosec team.

Highlight quantifiable improvements that show the risk reduction outcomes your for your organization at the next meeting.

# One final recommendation.



Before you start your next board presentation, take a step back and think about what it is that your board of directors really want to know and then align your discussion of risk with the company's strategic goals.

## CONSIDER:

- Are you presenting good or bad news? Do you want the board to feel happy about the progress Infosec is making? Or is this bad news because you don't have funding for everything that absolutely needs to be done?
- How happy do you want them to feel? Excited because cybersecurity posture is indeed better? Mildly concerned that some risks are manifesting but you have them under control? Or deeply concerned because there are "someone might go to jail-level" security holes?

Focusing your presentation to answer these questions is the key to a successful presentation.

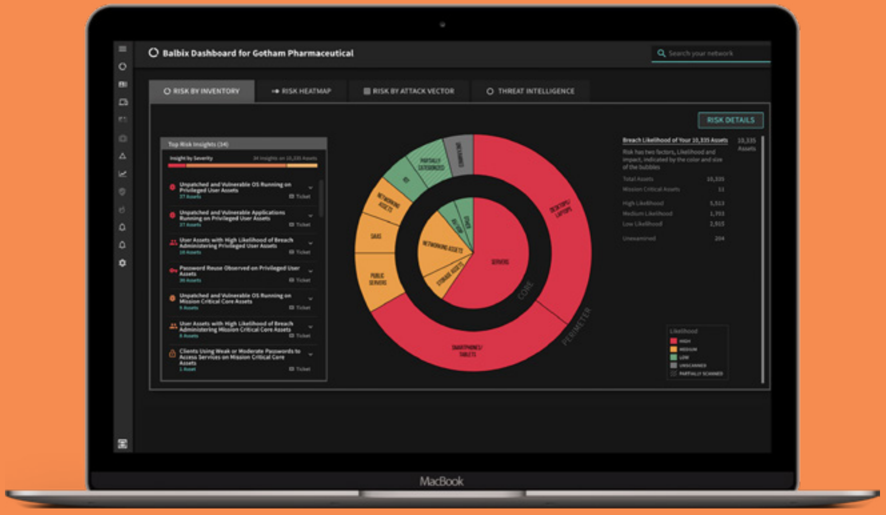
# Get a comprehensive picture of your security posture

Balbix can help you get a single, comprehensive, up-to-date picture of your cybersecurity posture.

Our AI-powered platform automates the continuous discovery of your assets, on-prem or in cloud, managed and unmanaged, and analysis of these devices across 100+ attack vectors. Balbix helps you estimate risk, likelihood, and impact scores for every area of your business and provides intuitive visualizations for your presentations to the board and C-suite colleagues. Balbix also provides prioritized fixes for improving your security posture and integrates into your vulnerability and risk management workflows. With Balbix, the board presentation that would've taken weeks to create can be completed in minutes.

Balbix®

REQUEST A DEMO TO LEARN MORE


Balbix Dashboard for Gotham Pharmaceutical
Search your network
RISK BY INVENTORY
RISK HEATMAP
RISK BY ATTACK VECTOR
THREAT INTELLIGENCE
RISK DETAILS
Top Risk Insights (34)
Insight by Severity
Unpatched and Vulnerable OS Running on Privileged User Assets
Unpatched and Vulnerable Applications Running on Privileged User Assets
User Assets with High Likelihood of Breach Administering Privileged User Assets
Password Reuse Observed on Privileged User Assets
Unpatched and Vulnerable OS Running on Mission Critical Core Assets
User Assets with High Likelihood of Breach Administering Mission Critical Core Assets
Clients Using Weak or Moderate Passwords to Access Services on Mission Critical Core Assets
Ticket
SERVERS
NETWORKING ASSETS
STORAGE ASSETS
DESKTOPS/LAPTOPS
SMARTPHONES/TABLETS
PUBLIC SERVERS
SAAS
IOT
PARTIALLY CATEGORIZED
UNCLASSIFIED
CORE
PERIMETER
Breach Likelihood of Your 10,335 Assets
Risk has two factors, Likelihood and Impact, indicated by the color and size of the bubbles
Total Assets
Mission Critical Assets
High Likelihood
Medium Likelihood
Low Likelihood
Unexamined
Likelihood
HIGH
MEDIUM
LOW
UNSCANNED
PARTIALLY SCANNED
MacBook

DOWNLOAD A SUGGESTED TEMPLATE FOR YOUR BOARD PRESENTATION HERE

THREE LAYERS OF INFORMATION RISK MANAGEMENT
Internal Audit
Legal
HR
Compliance
Privacy
RISK BY BUSINESS AND ATTACK TYPE
RISK SNAPSHOT AND TREND
$17M
Risk
48%
Likelihood
$35M
Impact
There is a 48% chance that we will have an impact of $35M from a cybersecurity event this year.

- 9 customizable slides
- Detailed guidance on how to tell a compelling story
- Additional slides to show connection between  information and risk