How CISOs gain trust in the Boardroom

“

By 2020, 100% of large enterprises will be asked to report to their board of directors on cybersecurity.

Gartner, *“The Comprehensive Guide to Presenting Risk and Information Security to Your Board of Directors”*

KUDELSKI SECURITY

The CISO Challenge

Embrace a Strategic Vision

Meet enterprise objectives

Enable strategic business initiatives

Strategic vs. Operational

Instill Confidence in Security Program

Effective security program & organization

Cyber strategy based on collaboration with business leaders

Build Executive Presence and Influence

Clear communication

Demonstrate progress

Risk-management language

KUDELSKI SECURITY

Get Insights on What Interests and Worries Boards the Most

Research conducted in 2018 through Kudelski Security's CISO Community initiative

- Joint engagement with Kudelski Security's **Client Advisory Council**
- Focus: **Board awareness** of the cyber challenges
- Sample Group: Over **80 CISOs**
- Goal: Board **Understanding** and **support** increases, confidence in the CISOs improves
- Executive Briefing: Cyber Board Communication & Metrics – **top challenges, recommendations**

KUDELSKI SECURITY

Summary of Findings

Top-5 Most Frequent & Challenging Questions Asked by Boards

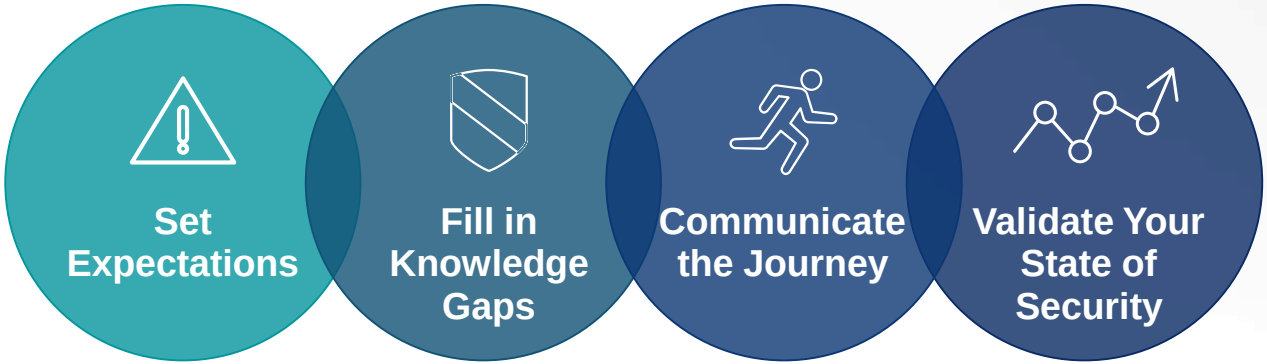
1. Are we secure?
2. How do we know if we've been breached?
3. How does our security program compare to peers within our industry?
4. Do we have enough resources for our cybersecurity program?
5. How effective is our security program, and is our investment properly aligned?

KUDELSKI SECURITY

Are we secure?

10-20 hours CISOs spend preparing a response to this question

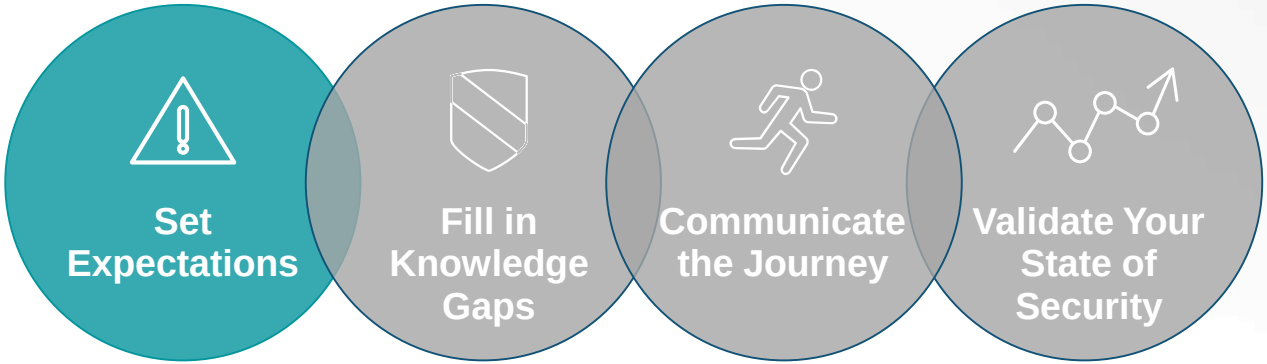
Response strategies:



Are we secure?

10-20 hours CISOs spend preparing a response to this question

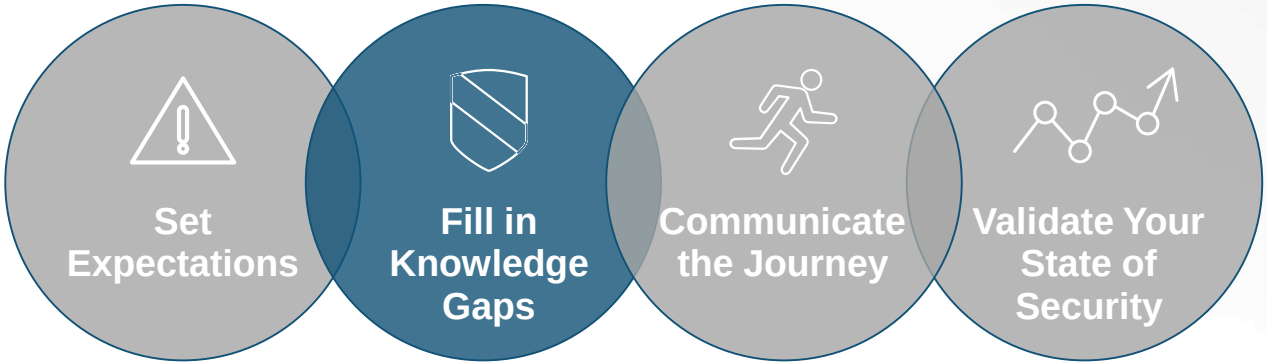
Response strategies:



Are we secure?

10-20 hours CISOs spend preparing a response to this question

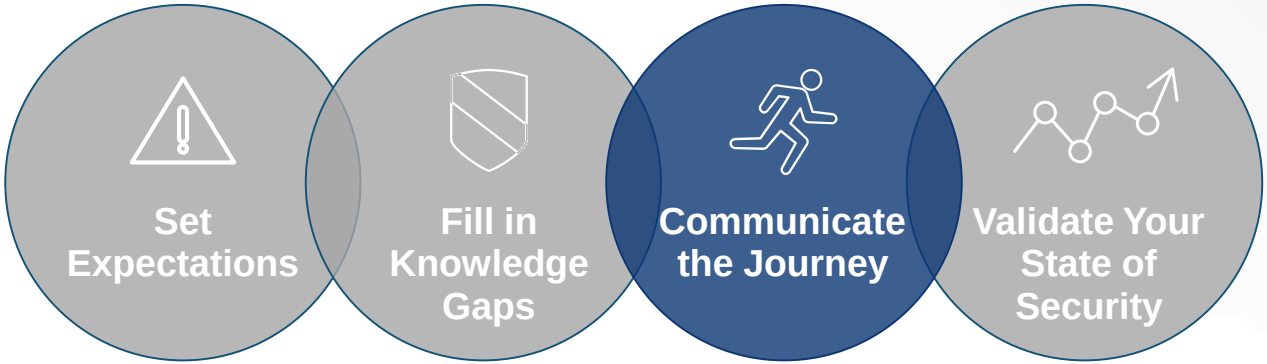
Response strategies:



Are we secure?

10-20 hours CISOs spend preparing a response to this question

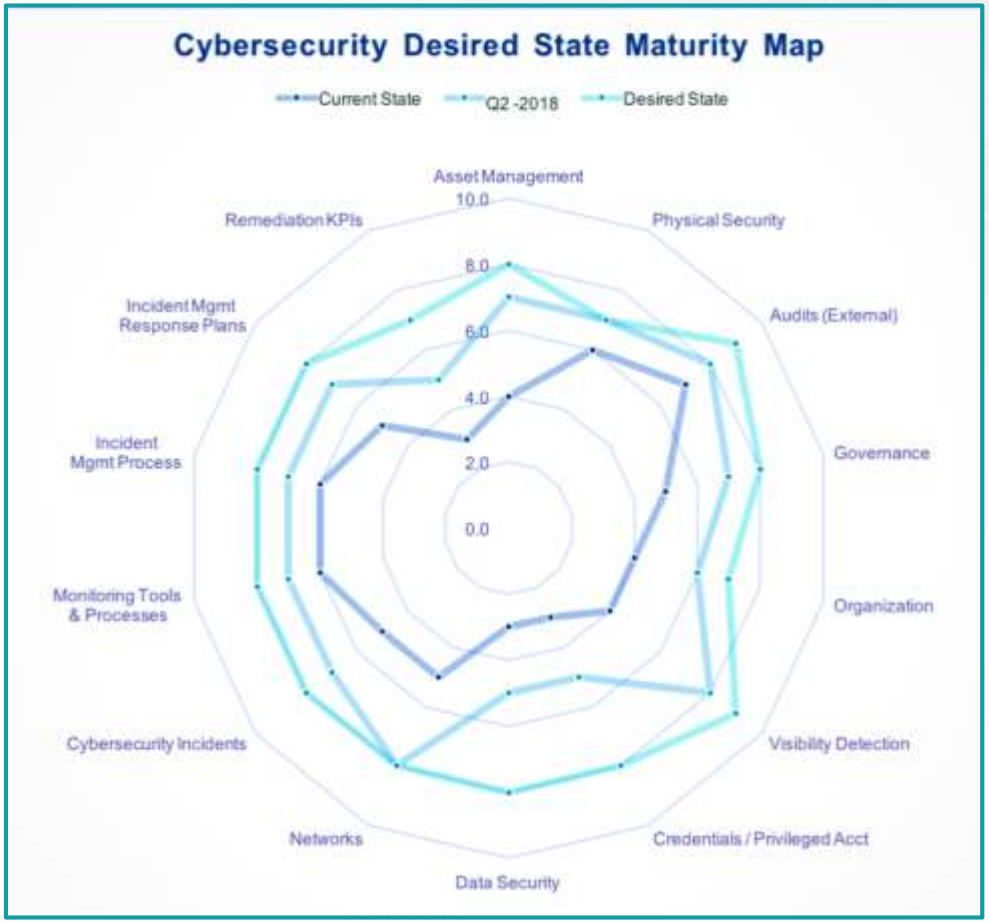
Response strategies:



Communicate the Journey

Example:

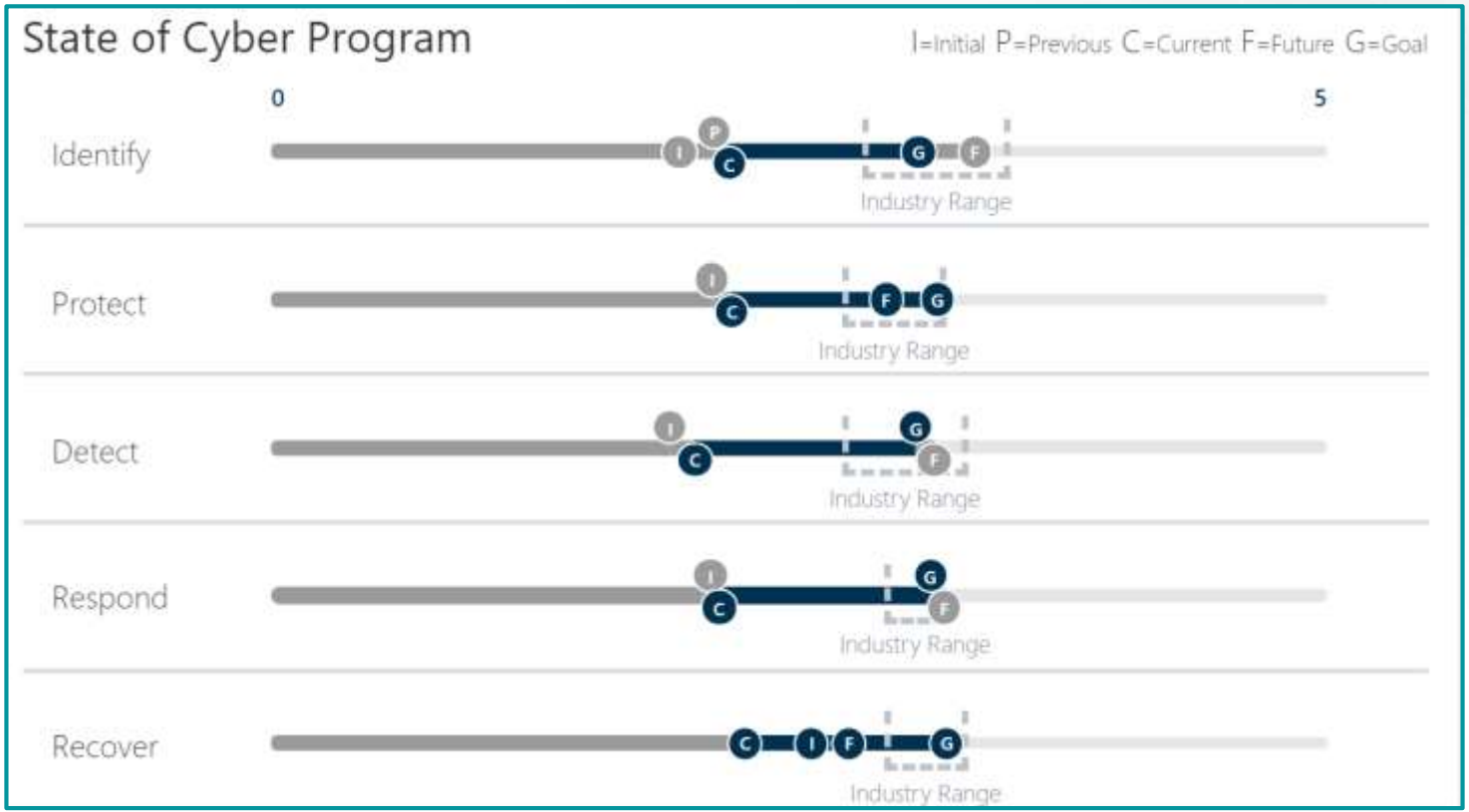
A **spider graph** provides an instant visual overview



KUDELSKI SECURITY

Communicate the Journey

Secure Blueprint SaaS provides out-of-the-box executive dashboards

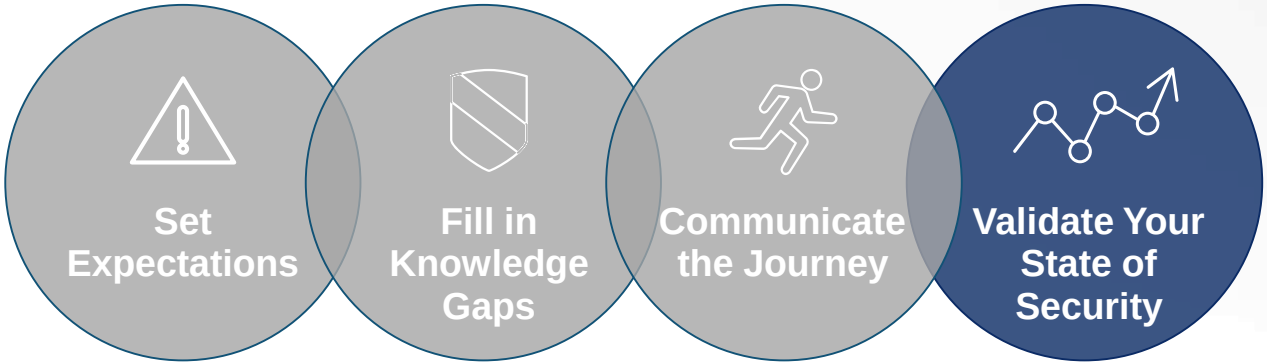


KUDELSKI SECURITY

Are we secure?

10-20 hours CISOs spend preparing a response to this question

Response strategies:



Validate Your State of Security

Effective Metrics

Quantitative	Qualitative
MTTD / MTTR	Risk reduction as outcomes of initiatives
Monitoring metrics	
Control efficiency	Accepted risks
Cyber hygiene	Dwell time reduction

*"Your ability to **respond and recover** is equally important to how **secure** you are"*

Ginny Davis, CIO and CSO

technicolor

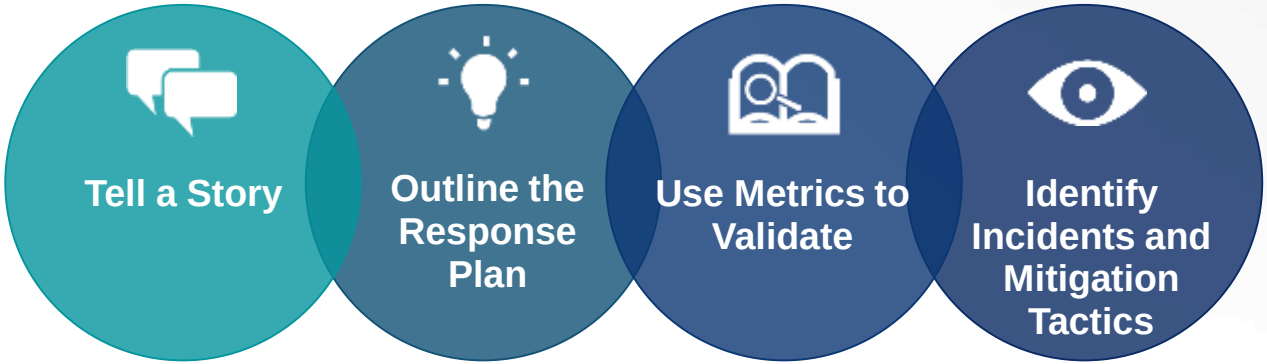
*"**In a perfect world, the absolute metric for a CISO** to have is the MTTD/MTTR of a more targeted attack." Pete Naumovski, VP and CISO*

BlueCross BlueShield Association

KUDELSKI SECURITY

How do we know if we've been breached?

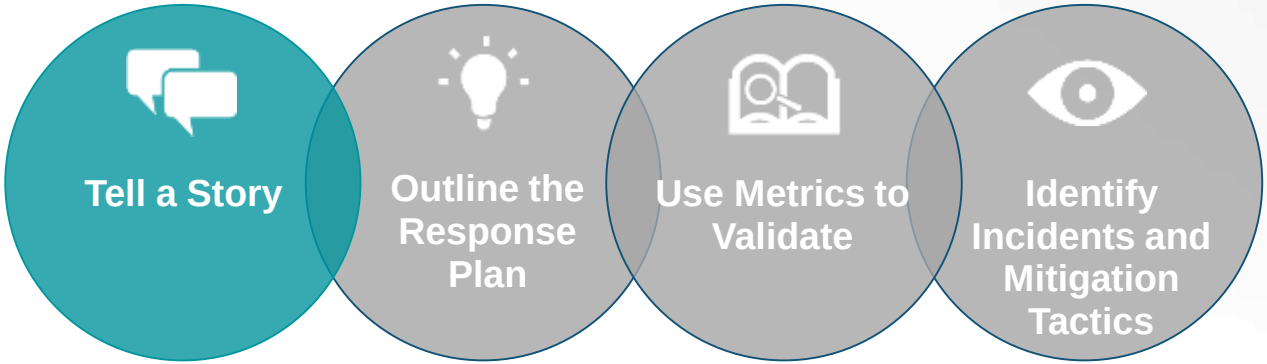
Response strategies:



Board members want confidence that the **response** to any breach is **crisp and effective**

How do we know if we've been breached?

Response strategies:



Board members want confidence that the **response** to any breach is **crisp and effective**

Tell a Story

A Storyboard Example

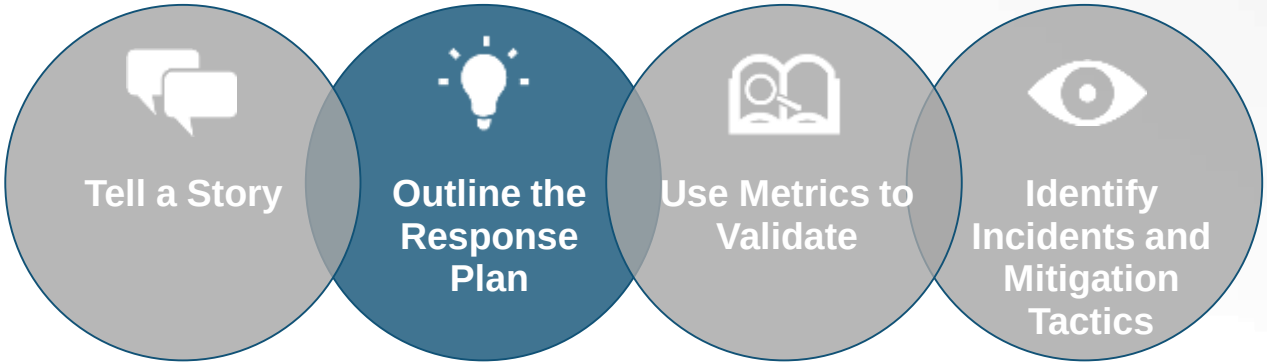
Mapping the anatomy of a high-risk attack to the security measures in place

Capability	Equifax Breach	Our Security Measures
Identify	Assets compromised	1. Sensitive data encrypted 2. Privacy technologies in place
Protect	Infiltrated through a flaw in Apache Struts tool	1. Timely patching 2. Periodic security assessments
Detect	Exploit of the Apache struts tool vulnerability to gain system access	
Respond	Late disclosure	Timely disclosure planned-for within our Incident Response plan
Recover	Potential identity theft to increase over the years	

KUDELSKI SECURITY

How do we know if we've been breached?

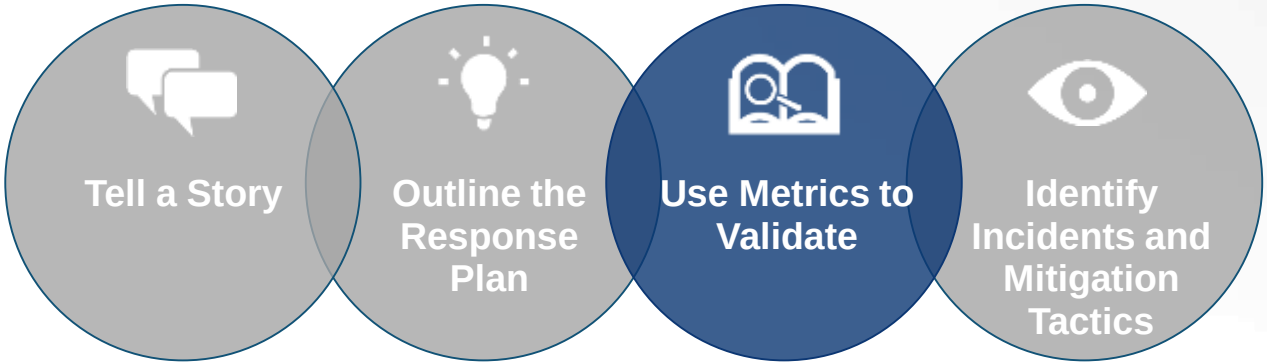
Response strategies:



Board members want confidence that the **response** to any breach is **crisp and effective**

How do we know if we've been breached?

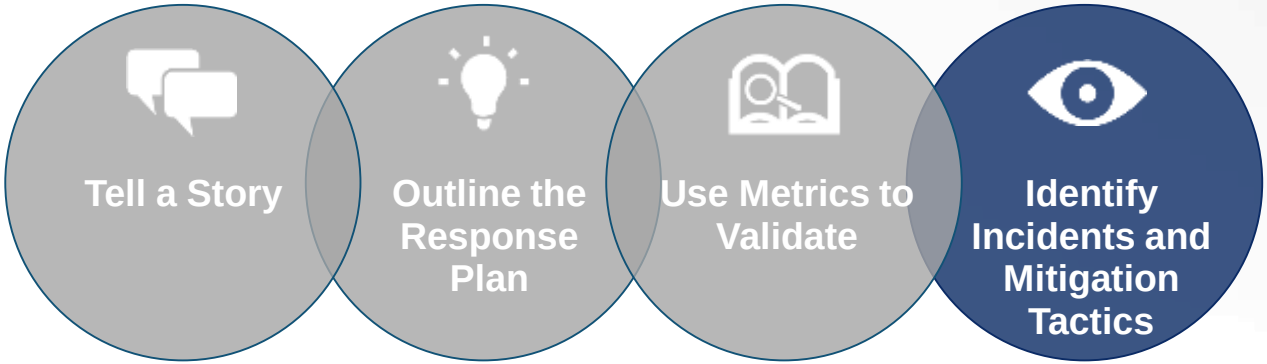
Response strategies:



Board members want confidence that the **response** to any breach is **crisp and effective**

How do we know if we've been breached?

Response strategies:

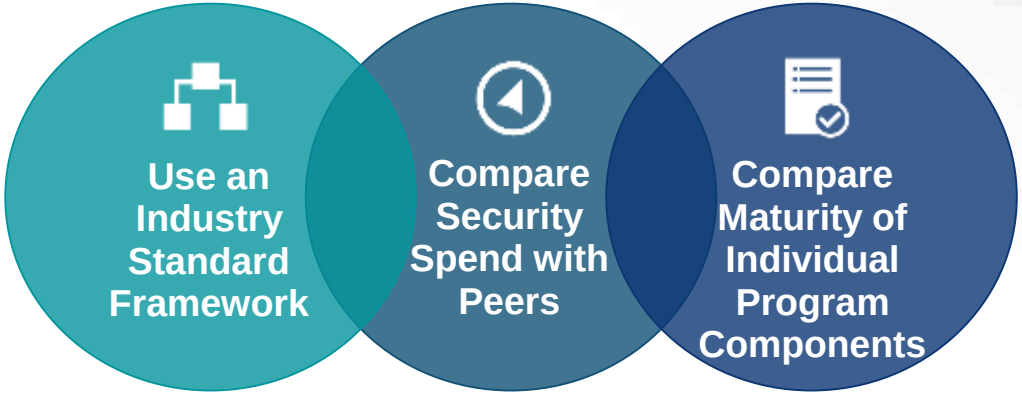


Board members want confidence that the **response** to any breach is **crisp and effective**

3 How does our security program compare to peers within the same industry?

NIST CSF
ISO 27xxx
most popular frameworks to measure maturity

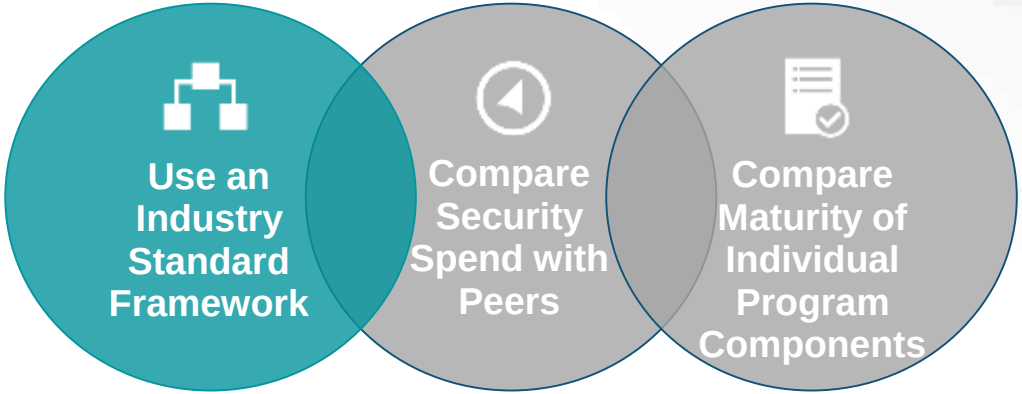
Response strategies:



3 How does our security program compare to peers within the same industry?

NIST CSF
ISO 27xxx
most popular frameworks to measure maturity

Response strategies:

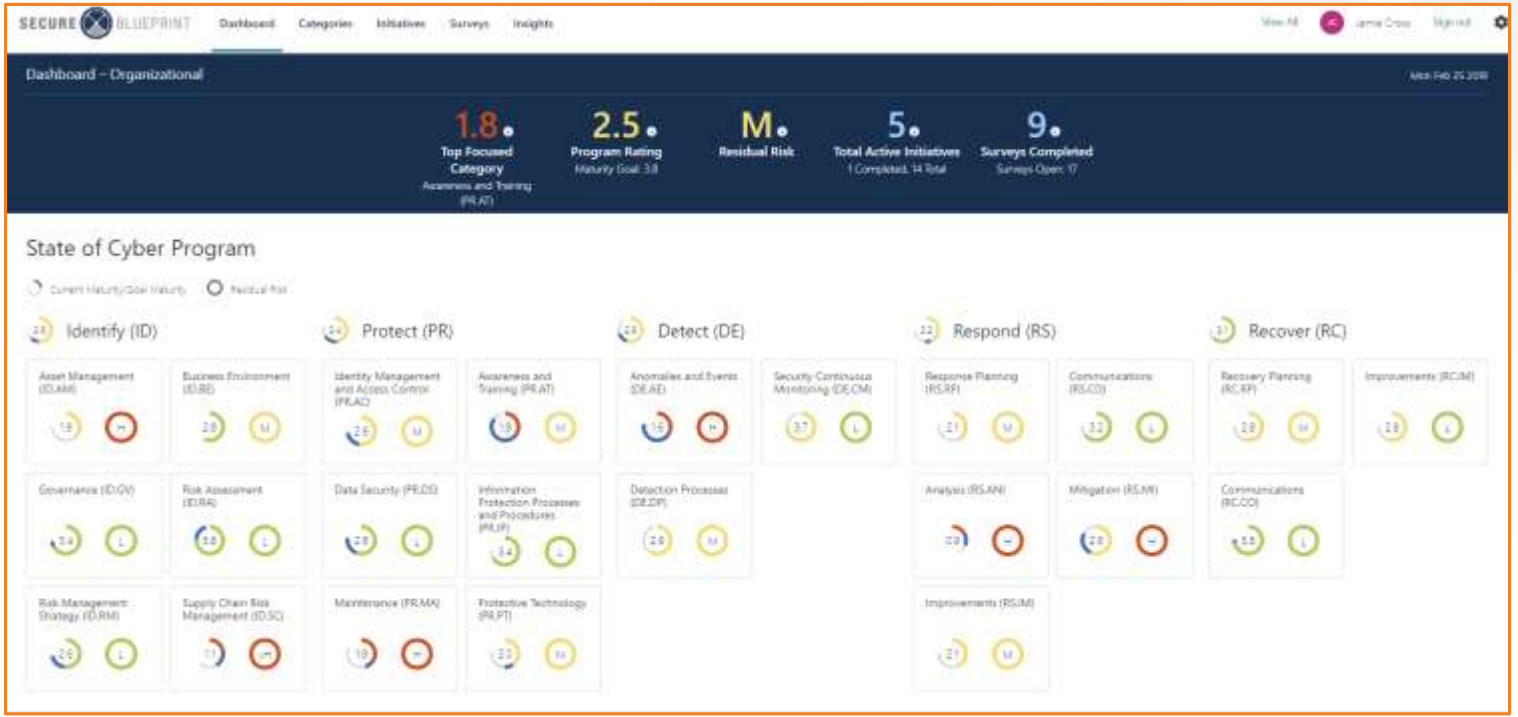


Benchmark your security program's maturity with an industry-standard framework

Secure Blueprint SaaS provides an ongoing view of your program's risk and maturity scores

Frameworks

- NIST CSF
- Cyber Portfolio Maturity Model (CPMM)

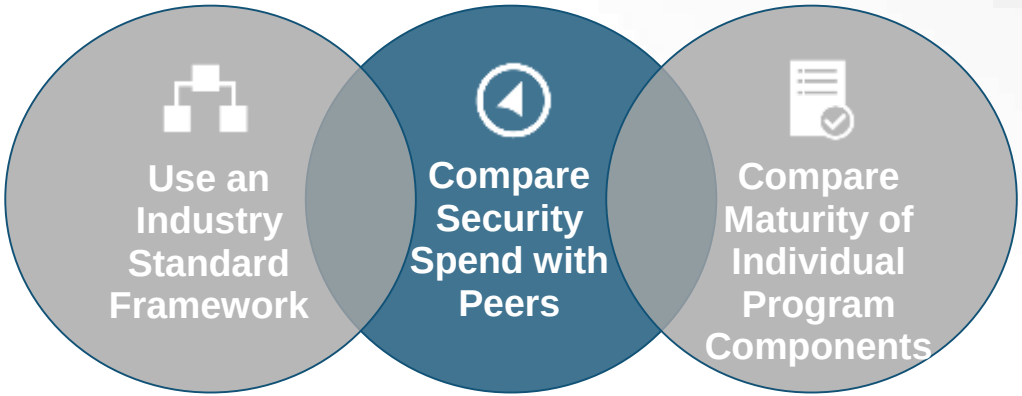


KUDELSKI SECURITY

3 How does our security program compare to peers within the same industry?

NIST CSF
ISO 27xxx
most popular frameworks to measure maturity

Response strategies:



Compare Security Spend with Peers

Suggested channels for benchmark data

EXAMPLE

Industry-specific cyber community

Meet monthly

Get updates on industry cyber trends

Compare programs and maturity

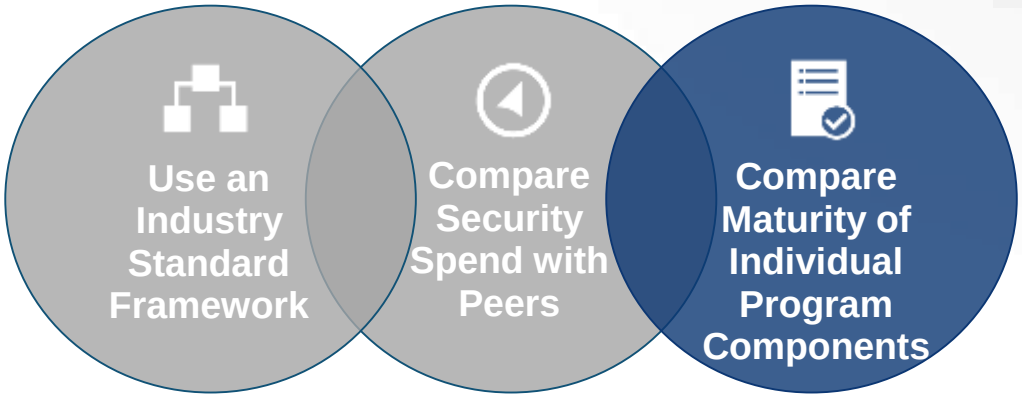
Share latest incidents

KUDELSKI SECURITY

3 How does our security program compare to peers within the same industry?

NIST CSF
ISO 27xxx
most popular frameworks to measure maturity

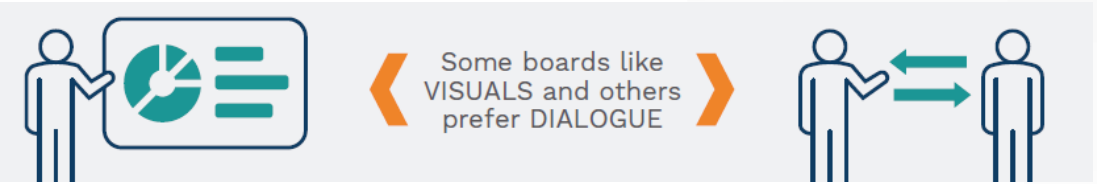
Response strategies:



Advice from Council members to Improve Board Communication

Long Term Focus

- Create a presentation that will **resonate** with *your* board
- **Educate** and address misunderstandings **(compliance ≠ secure)**
- **Engage** the board to help push security to the entire enterprise



"Have onboarding conversations with new board members, share the latest board presentation and metrics" *Robert Drawer, Global Director of IS* MAYER·BROWN

KUDELSKI SECURITY

Advice from Council members to Improve Board Communication

Board Meeting Content

1. Metrics Research

- **Ask** boards
- **Review** company reports to understand business objectives
- **Present** metrics that don't take long to capture
- **Use** factual information only

2. Focus on Context

Provide the **bigger picture**, show business alignment

"Always have data to back up your recommendations. Stay away from opinions."

Tony Spinelli, former CISO

KUDELSKI SECURITY

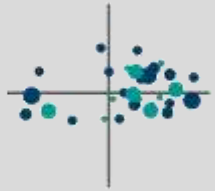
Advice from Council members to Improve Board Communication

Board Meeting Content

Focus on Strategic elements - create a story that shows:

- Security and investments align **to business priorities**
- Controls are **effective**
- Your investment outcomes **enable business**
- Your plan is **backed up by data** and **aligned to a maturity model**
- Prioritized program areas and **benchmarks with peers**

Effective visual displays



Building Board Presentations

Findings Summary

- **Frequency:** **Quarterly**, with annual deep dives
- **Length:** **30 minutes**, but have a Plan B that is 10-15 minutes
- **Prep Time:** Allow **45 to 80 hours** for each presentation over 2-3 weeks
  5 to 25 revision cycles as part of the internal review process
- **Slides:** Limit to **5-7 slides** (two slides in case of time shortage)

KUDELSKI SECURITY

CISO advice for building board presentations

Cyber reports for Boards typically include five sections:

Situational Awareness

Present current and emerging industry trends, their relevance to the board. Show how to mitigate risks

Incident Response

Present noteworthy incidents, how they were handled, and the controls in place you found helpful

Risk/Threat Lens

Present the organization's risk appetite, the critical & unresolved security risks, remedial action and the residual risk following remediation

Capability Maturity Aligned to a Common Framework

Measure maturity across all entities. Show weaknesses and trends

Strategy (2 slides)

First, a refresher on program drivers and capabilities, and then an **18-month outlook** how the program is moving toward the goal. Demonstrate progress, alignment, and continuous improvement

KUDELSKI SECURITY

Send supporting materials and presentation for boards to review prior to the meeting

"Before presenting to the board, get buy-in from one person in the meeting who will support what you are presenting"

Robert A. Drawer, Global Director of IS

MAYER·BROWN

KUDELSKI SECURITY

KUDELSKI SECURITY

Thank You

Shiri Band

Global Solutions Marketing