



CISO PERSPECTIVES

What Top CISOs Include in Updates for the Board

Exclusive Insights from the RSAC Executive Security Action Forum (ESAF)

A Message from the RSAC ESAF 2022 Program Committee

As a forum for candid discussion among peers, ESAF sessions are confidential, invitation-only discussions typically limited to about 100 CISOs. With our 20th anniversary approaching, the ESAF community would like to provide some of our hard-earned wisdom to the larger RSAC community through a series of reports on topics of interest to all information security executives. Our goal is to help all organizations improve the management of cyber risks.

For more information on ESAF, see www.rsaconference.com/ESAF

The RSAC ESAF 2022 Program Committee includes:

- Justin Acquaro**, Chief Information Security Officer, Evernorth (Cigna Corporation)
- Brad Arkin**, Senior Vice President, Chief Security and Trust Officer, Cisco
- Jason Barnett**, Vice President, Chief Information Security Officer, HCA Healthcare
- Chris Betz**, Chief Information Security Officer, Capital One
- Jerry Geisler**, Senior Vice President and Chief Information Security Officer, Walmart
- Richard Hale**, Global Chief Information Security Officer, Sony Group Corporation
- Gary Harbison**, Global Chief Information Security Officer, Bayer
- Katie Jenkins**, Executive Vice President for Global Cybersecurity and Chief Information Security Officer, Liberty Mutual Insurance
- Michael Johnson**, Chief Information Security Officer, Meta Financial Technologies, Meta Platforms
- Robert Martin**, Chief Information Security Officer, Alberta Health Services (AHS)
- Catherine McCully**, Chief Information Security Officer, Procter & Gamble
- Michael McNeil**, Senior Vice President, Global Chief Information Security Officer, McKesson
- Vishal Salvi**, Global Chief Information Security Officer & Head of Cyber Security Practice, Infosys
- Emma Smith**, Chief Information Security Officer, Vodafone
- JR Williamson**, Senior Vice President and Chief Information Security Officer, Leidos

RSAC[®]
Executive Security
Action Forum

A Community of Fortune 1000 CISOs

About RSAC ESAF

The Executive Security Action Forum (ESAF), an RSA Conference (RSAC) community, has been a trusted forum for Fortune 1000 security executives since 2003. Led by a program committee, the community shares information at invitation-only, confidential sessions throughout the year and at their annual meeting at RSA Conference. RSAC ESAF enables security leaders at some of the world's largest enterprises to collaborate and find actionable solutions to common challenges.



Contents

- A Rare Glimpse Inside Actual Board Updates 4**
- Overview: Common Threads and Different Approaches 5**
- How Updates Are Organized 6**
- Conveying Risk 7**
 - Board Objectives for Understanding Cyber Risk Management 7
 - Communicating Aspects of Risk Management 7
- Maturity Scores 11**
 - Why Include a Maturity Score? 11
 - Limitations of Maturity Scores 11
 - Scores That Measure Efficacy 11
- Metrics 12**
 - Why Include Metrics? 12
 - What Metrics CISOs Report 12
 - Meaningful Metrics 13
 - Metrics That Are Not Meaningful 13
- Reporting on Significant Incidents 14**
- Providing Updates on Security Initiatives 15**
- Conclusion 16**
- Appendix I: Examples of Tables of Contents for Board Updates 17**
- Appendix II: Examples of Charts and Diagrams 18**
- Appendix III: Metrics Included in Board Updates 27**
- Appendix IV: Examples of Metrics Dashboards 28**
- Appendix V: RSAC ESAF 2022 Program Committee Biographies 31**

A Rare Glimpse Inside Actual Board Updates

Cyber risk gets attention at the top levels of global companies today; it is seen as a strategic risk that could significantly impact the business. Keeping the board updated on how the company is managing cyber risk is one of the most important aspects of a CISO's job.

CISOs often discuss ways to effectively communicate with boards. However, they rarely have the opportunity to see the content of board updates at other companies.

This report explores in depth what top CISOs include in updates to the board and why. It delves into the thinking behind these crucial decisions, as described by some of the world's foremost enterprise security leaders.

Research Methodology

The ESAF Program Committee guided the analysis and provided direction for the research. The quotes throughout the report are their reflections on the topics.

The research is based on materials from actual, recent board updates contributed by eight anonymous CISOs. In follow-up interviews, they shared more details on their practices and commented on materials submitted by others. The contributors represent a cross-section of members from the ESAF community and are from seven different industries.

To ensure confidentiality, all research findings were anonymized. This enabled candid sharing of examples and opinions for the benefit of the broader community.

“ Even for the most experienced CISOs, going to the board is an area they invest time and effort in—no one is complacent about how these meetings go. ”

Emma Smith
CISO, Vodafone



How to Use This Report

This report is derived from actual materials that CISOs present to their boards. It contains numerous anonymized examples of written content, dashboards, charts, and diagrams (with notional data).

It is intended as food for thought, providing ideas to use in developing updates for the board. It is *not* intended as a playbook, a set of best practices, or an industry standard for reporting to the board.



Overview: Common Threads and Different Approaches

The CISOs in our research all include the following topics in their updates:

- **Changes to the risk landscape**

Generally focused on threats, while also covering regulations and contractual obligations

- **Priority risks**

What cyber risks and/or risk factors are highest priority

- **Maturity score**

An overall score reflecting the company's security maturity and/or security posture

- **Security initiatives**

Progress of specific security initiatives

- **Security incidents**

Significant security incidents that affected the company

Although there are common topics in updates, the level of emphasis and approach to the topics varies considerably—particularly for the topics of *risk* and *metrics*.

Variations are driven by differences in board expectations, regulatory environments, vertical industry, business objectives, and CISO perspective. Even within a company, the approach to cyber risk updates may shift over time to reflect the preferences of board members, the maturity of the security organization, and the evolving CISO-board relationship.



“ Where CISOs can lose credibility is to go in with an overly positive report. If you only show them a rose garden, you are going to leave them wondering if it’s really that good. You want to be transparent by reporting on the good things and the gaps. ”

Jerry Geisler
SVP and CISO, Walmart



How Updates Are Organized



This report amalgamates content that CISOs deliver in various contexts:

- Materials that are provided to either a board committee and/or the full board
 - The CISOs in our research typically update a board committee¹ quarterly and the full board annually. (In this report, “the board” is used for both audiences.)
 - Usually updates for committees are longer and more detailed. For instance, in terms of presentation time, a CISO may get 30 minutes with the board committee and 10 minutes with the full board.
- Materials that CISOs give boards in a presentation/memo, pre-read, or appendix
 - Often, the format of an update is a brief summary plus an appendix. For instance, the CISO may provide a three-page summary with a 30-page appendix including details and metrics.

The flow of topics varies between CISOs:

- Some choose to start with external issues, such as changes to the threat landscape, others with the status of the security roadmap.
- Various ways of ordering the topics are shown in [Appendix I: Examples of Tables of Contents for Board Updates \(page 17\)](#).

The topics covered also vary for an individual CISO:

- Some topics may not be covered every quarter but rather annually or semi-annually. For example:
 - A “board education” item is on the agenda twice a year.
 - An overview of the cybersecurity strategy is covered once per year.
- Topics change to reflect recent events such as the completion of a project or an incident at a third party.

While topics can change, several CISOs emphasized the importance of ensuring continuity and consistency over time. They look at updating the board as an ongoing conversation.

“ A good way to start is by updating the board on the commitments you made in the previous meeting, ‘Here’s where we left off in the last discussion,’ That way it’s progressive. ”

Jason Barnett
VP, CISO, HCA Healthcare



¹ Board committees that CISOs report to include the Audit Committee, Risk & Technology Committee, Nominating and Governance Committee, Compliance Committee

Conveying Risk

Board Objectives for Understanding Cyber Risk Management

For conveying risk, the CISOs we spoke to consider the board's objectives for understanding how cyber risk is being managed at the company. The board's objectives include:

- **Ensure risks are managed with due care.**
This is the fiduciary responsibility of boards.
- **Demonstrate they have been providing oversight.**
They need to know and understand the gaps and be able to show they were in on the details, not just getting top-level reporting.
- **Hold the CEO and executive leadership at the company accountable for managing risk.**

Legal Defensibility

If an incident occurs, there is the potential for legal action against board members.

To put themselves in a defensible position, board members need to be able to show that they were adequately overseeing cyber risk management, including ensuring that risks were being addressed and prioritized in a reasonable way.

Communicating Aspects of Risk Management

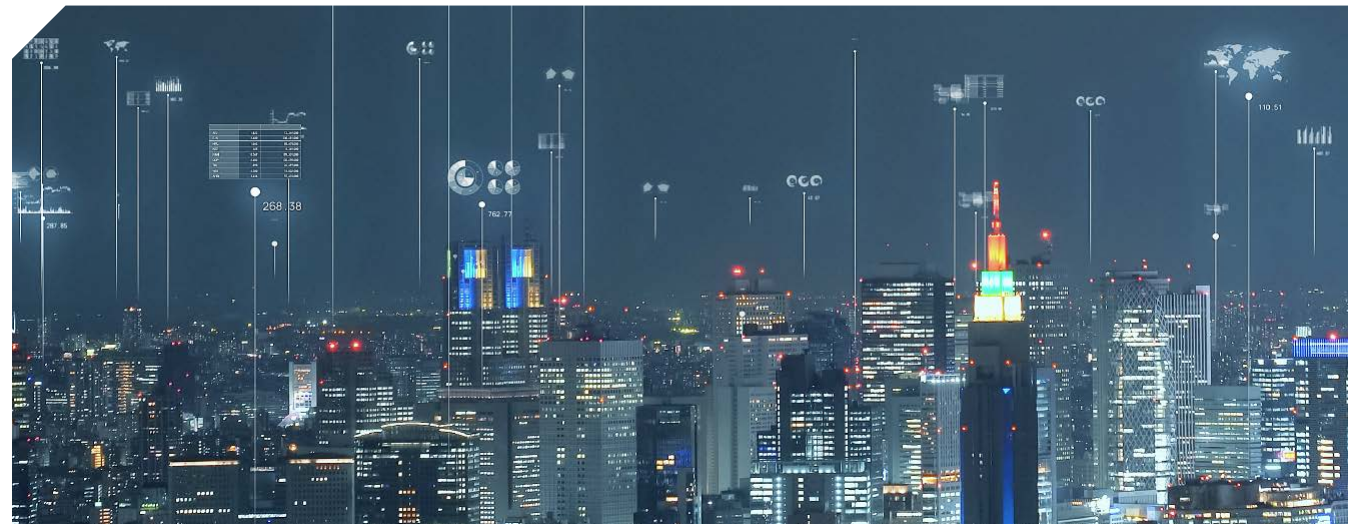
In our research, risk management is discussed in board updates from various angles, demonstrating to the board that:

- The risk landscape is monitored.
- Risks are analyzed and prioritized.
- Risks are being mitigated/reduced.
- Risk appetite is being factored into cyber risk management decisions.
- Cyber risks are included in overall enterprise risk management (ERM).

Often, multiple angles are combined in a single slide or story. For instance, statements about escalating risks are often combined with descriptions of plans to mitigate those risks.

“ Boards look at cyber risk in the context of the company's overall culture. The cyber risk conversation depends on what the company values. If the company is driven by cost optimization, it's about return on investment. If the company is more growth oriented, it's about enabling the next big idea. ”

Chris Betz
CISO, Capital One



Risk Landscape

Changes to the risk landscape that are covered in board updates include changes in:

- **Cyber threats.** For example:
 - Current, emerging, and future threats
 - New attack vectors
 - Specific threat actors and their methods
 - How trends are impacting the organization, the industry, and suppliers
 - Metrics on the volume of threat activity
- **Vulnerabilities of greatest concern**
- **Regulation/oversight.** For example:
 - Information on new or upcoming regulations, industry standards, and/or contractual obligations
 - Metrics on engagements with regulators, customers and auditors
- **Readiness**
 - Measures in place or planned to mitigate threats

“ When you talk about threats, what the board really wants to know is how prepared is the company to deal with them – readiness, resiliency, and business continuity. Otherwise, you’re just admiring the problem. ”

JR Williamson
SVP and CISO, Leidos



Risk Analysis/Prioritization

When relaying how risks are being analyzed and prioritized, CISOs use various methods based on their sense of what will work for their board. The CISO may present, for example:

- **List of top risks**
 - Statements of risk in a bulleted list
 - Descriptions of risks and risk reduction measures
- **Risk scores represented on a heatmap**
 - Estimates of the likelihood and impact of each risk
- **Depictions of higher risk areas**
 - Risks by market or product areas
 - Requires managing the sensitivities around identifying areas of the company with poor risk posture. Security collaborates with the business leaders ahead of time, working together on what will be presented to the board.
- **Descriptions of risk scenarios**
 - Results of threat modelling, pen tests, and/or tabletop exercises
- **Details on how certain risks are being managed**
 - A deeper dive about certain risks the board is interested in, e.g., supply chain risks

In some cases, security teams use risk scoring systems internally to prioritize their efforts but do not find it useful to share those numbers with the board.



EXAMPLE CHARTS & DIAGRAMS:

Emerging/Future Threats Mapped to Plans for Controls – [Page 18](#)

Cyber Risk Management: Top 5 Risks and Countermeasures – [Page 19](#)

Heatmap: Top Cyber Risks with Inherent vs. Residual Risk – [Page 20](#)

Market Risk Scorecard: Status of Controls in Each Country – [Page 21](#)

Security Posture: Product Risks by Business Unit – [Page 21](#)

“ Risk statements should be in terms of business impact. If you state the risk as ‘script injection,’ that means nothing to a board member. But if you say, ‘Our systems would be inoperable because of a cyber attack,’ that makes sense. It resonates more with a board member. ”

Justin Acquaro
CISO, Evernorth



Is the board presented with risk quantified in financial terms?

The board updates in our sample did not present cyber risks quantified in financial terms except in the context of the enterprise risk management program (see following page).

However, CISOs convey the financial significance of cyber risks in various ways. For instance, they may:

- Present a dashboard of company “zones” (business units or projects) showing the amount of revenue each zone generates and describing the cyber risk level of each zone. This gives the board a sense of how much revenue is exposed to each level of cyber risk.
- Do a detailed assessment each year on a severe-but-plausible risk scenario and quantify the financial losses of that scenario. This is done primarily for insurance purposes and the results are shared with the board.

Most CISOs in our research who have evaluated building a capability to quantify cyber risk in dollar values found that the resources and talent required would be prohibitive. For example, a successful program would involve hiring a team of actuaries, which is typically out of reach for most security teams.

Risk Mitigation/Reduction

The CISOs in our research discussed risk mitigation/reduction from various angles including:

- **Trends in key metrics**
 - For example, to show third-party risk is being reduced, a CISO could include current and historical metrics on suppliers’ security ratings.
- **Controls strategy**
 - Describing layered controls helps to allay concerns from the board around narrow issues such as whether 100% of servers are patched.
- **Security Roadmap**
 - Discussions of risk reduction are in the context of making progress implementing an overall plan to meet target maturity levels.
- **Gaps**
 - Some updates show specific gaps in controls and strategies to address the gaps.
- **Cost to mitigate**
 - Plans for mitigating specific risks are sometimes discussed with cost estimates, e.g., “This is how much we’re spending to mitigate this risk.”
 - Costs for cyber insurance.



EXAMPLE CHARTS & DIAGRAMS:

Security Transformation Roadmap – [Page 22](#)

Risk Mitigation: Inherent Risks Reduced Through Layered Controls – [Page 23](#)

“ In interactions with the CISO, what the board wants to know is: Does the organization have the right leader? Does the leader have the right plan? And is the plan appropriately resourced? ”

Brad Arkin
SVP, Chief Security and Trust Officer,
Cisco



“ Cybersecurity has a lot of technical jargon. For describing risk to the board, think about how to translate it into layman’s terms. Will someone without cybersecurity expertise understand this? ”

Catherine McCully
CISO, Procter & Gamble



Cyber Risk Appetite

The CISOs in our research described ways to gauge the risk appetite of the company and integrate it into measurements for cybersecurity. They emphasized that risk appetite is not something the CISO can figure out in a silo.

Some companies write statements of cyber risk appetite. These could be developed by, for example, the CISO and governance/risk/compliance officers, sometimes with the involvement of board members. Based on the written statements, the CISO sets targets for metrics, maturity scores, etc.

At most companies however, instead of formal written statements, risk appetite is communicated through day-to-day conversations between the CISO and other executives. The CISO gains an understanding of the company's risk appetite and then uses it to set targets.

Once the targets are set, to bring the board into the risk appetite discussion, one approach is to present the targets to the board and seek feedback.

Enterprise Risk Management (ERM)

For the company's ERM program, the board is typically provided with a representation of overall enterprise risks, e.g., an enterprise risk registry or heatmap. Aggregate or significant cyber risks are included in this big picture of enterprise risks using the same format and measurement scales. This way, cyber risks can be compared to other types of risks such as market or operational risks. For the companies in our research sample, quantifying cyber risks for the ERM program is either the responsibility of the CISO or a separate risk team.

“ For really engaging the board in a conversation around cybersecurity and risk appetite, consider moving the focus away from metrics. Storytelling can be more effective for educating and garnering feedback on approaches and outcomes. ”

Katie Jenkins
EVP for Global Cybersecurity and
CISO, Liberty Mutual Insurance



Example of a Risk Appetite Conversation with the Board

One way to converse with the board about risk appetite is to get their feedback on specific scenarios. For instance, a CISO presented an analysis with confidence levels (low, medium, high) for the company's ability to withstand the following types of attackers:

- Nuisance protester with limited skills
- Lone wolf actor looking to commit a fraud
- Organized criminal targeting businesses for material gain
- Sophisticated nation state mounting a widespread attack on an organization

The analysis also included estimates of the time and investment that would be needed to reach different levels of confidence. The board then provided feedback on the level of confidence they would like, given the investment required.



Maturity Scores

The updates we looked at all included a score from an assessment of the organization's enterprise security. Scores are often based on a maturity model or risk management framework such as the NIST Cybersecurity Framework (CSF), International Standards Organization (ISO) 27001, Information Security Forum (ISF), and/or industry-specific frameworks. This report refers to these scores as "maturity" scores, although not all CISOs use this term.

Most of the CISOs also include previous scores and/or industry scores for comparison.

"Over time, a maturity score helps the board understand whether the company is making progress towards its desired end state for security. It gives the board a comfort level that the security team is focusing on the right areas."

Michael McNeil
SVP, Global CISO, McKesson



Why Include a Maturity Score?

The CISOs pointed out that boards are interested in maturity scores because they:

- Provide a way to set targets and objectives for the security program
- Show how the security team is making progress over multi-year trends
- Demonstrate that the company's security practices are reasonable and in line with industry practices, within a framework that others would recognize
- Provide a way to compare the company's security program with other companies

Limitations of Maturity Scores

In our discussions, CISOs observed that depending on the assessment method, maturity scores may not give the board a meaningful sense of security posture. Assessments using the NIST CSF often don't measure the efficacy of controls but rather assess if the controls are in place, how broadly they are in place, and if there is a process to ensure controls are consistent/maintained/updated. For example, assessments might evaluate whether multi-factor authentication is in place but not whether it is effectively controlling access to critical resources.

Scores That Measure Efficacy

Given the limitations of maturity frameworks, some CISOs present NIST CSF maturity scores in conjunction with metrics or audit findings to give a more complete picture of efficacy.

Others combine and/or extend frameworks for a more meaningful measure of efficacy. Approaches include:

- Incorporating quantitative metrics, such as results of threat modelling and pen testing, into the scoring system.
- Bringing in external security experts with specialized knowledge on maximizing control effectiveness to both advise on leading-edge practices and to incorporate efficacy into the scoring system.

The trade-off in using customized methods is that the score might not be useful for comparing to companies that use a different method. In some cases, companies work with others in their industry to develop a common assessment methodology for comparable scores.

EXAMPLE CHARTS & DIAGRAMS:

Current State of Maturity – [Page 23](#)

Comparison of Maturity Scores with Peers – [Page 23](#)

Current vs. Target Scores for Security Objectives – [Page 23](#)

Metrics

There is some debate within the ESAF community about how to include metrics in board updates. Some CISOs find it is more effective to focus on narratives rather than numbers. Others put more emphasis on metrics.

Most board updates in our sample include at least a few metrics. We did not find a standard set of metrics that was reported by everyone.

The range of category names used by different CISOs suggests that they present metrics for different reasons. For instance, phishing click rate could be categorized as an indicator of “risk”, “maturity”, or “performance” depending on the CISO.

“ The challenge with metrics is that it depends on the board. Get in front of a different board and you’ll find they want different levels of detail every time. ”

Robert Martin
CISO, AHS



Why Include Metrics?

In our discussions around metrics, CISOs gave several reasons to regularly report metrics to the board:

- Metrics enable the board to track risk management over time, with hard data.
- Metrics give the board assurance that they have enough detail about security to perform effective oversight.
- The Internet Security Alliance in conjunction with the National Association of Corporate Directors (NACD) have published a widely used handbook for boards which says operational metrics can be helpful for “understanding critical compliance issues and stimulating useful discussions about trends, patterns, and root causes, and benchmarking with others in the industry.”²
- Seeing metrics reassures the board that the security team is tracking data and using it in its decision making.
- Including a set of metrics in every update provides a basic level of transparency about the security team’s performance.
- In the event of a breach, a history of consistent reporting around metrics provides defensibility that the board, management, and CISO had been fulfilling their duties.

What Metrics CISOs Report

To determine what metrics to include in board updates, the CISOs we spoke to choose metrics that:

- Reflect the company’s desired business outcomes and highest risks
- Could serve as key risk indicators so the board can track residual risk
- Interest the board
 - CISOs take cues from questions the board has asked in previous meetings. For example, if the board shows interest in an outcome of a security initiative, that becomes a metric going forward.
- Demonstrate the progress of security initiatives
 - Once an initiative is complete, the metric is no longer reported.
- Convey a risk threshold has been crossed
 - The CISO may monitor certain risk indicators and bring them to the board’s attention only when they exceed the board’s historic risk appetite.

CISOs often work with other executives, or in some cases a formal committee is formed, to determine what metrics to include in board updates.



EXAMPLES OF METRICS & DASHBOARDS

Metrics Included in Board Updates – [Page 27](#)

Metrics Dashboards – [Page 28](#)

² *Cyber-Risk Oversight: Key Principles and Practical Guidance for Corporate Boards*. 2020, p. 54.
<https://isalliance.org/isa-publications/cyber-risk-oversight-handbook/>

Meaningful Metrics

In our discussions, the CISOs described ways to formulate and present a metric that will be meaningful to the board:

- **Show trends.**
 - Trend data is more useful and impactful than a point-in-time metric.
- **Show targets.**
 - Setting targets for metrics is often a negotiation with the business, as targets involve cost and business trade-offs.
 - In many companies, targets are regularly adjusted to reflect the expectation for continuous improvement.
 - The board may give the CISO feedback on whether targets reflect the company's risk appetite, as described in the section on Risk Appetite on [page 10](#).
- **Convey the right message.**
 - A metric can be formulated to show either low numbers (5% phishing click rate) or high numbers (95% phishing non-click rate). In general, it is more intuitive for high numbers to be better.
 - However, when discussing an area in which security is relatively weak, the CISO might reinforce the need for improvement by presenting a low number rather than a high number.
- **Incorporate the company's security policies.**
 - For example: If the policy is to patch Priority 1 issues on servers within 24 hours, a metric could be "Percentage of servers patched within 24 hours for Priority 1 issues." This is more meaningful than "Percentage of servers that are fully patched."

- **Reflect priorities.** For example:
 - Scope a metric on application security to cover only the top 100 applications.
 - Scope a metric on supplier security to cover only Tier 1 suppliers.

Metrics That Are Not Meaningful

The CISOs also discussed types of metrics that would not be meaningful to their boards, including metrics that:

- **Require deep cybersecurity expertise.**
 - Board members may not volunteer that they don't understand a set of metrics.
- **Are too detailed for the board.**
 - In our research, there was no consensus on where to draw the "too detailed" line. For example, some boards are interested in metrics that show average time to detect/respond/mitigate/contain after an event, while other boards would have no interest in this level of detail.
- **Are based on insufficient data.**
 - For instance, if the company does not know what percentage of assets are being regularly scanned, a metric on scan findings might not be meaningful.
- **Reflect outdated security strategies like the perimeter model.**
 - For example, metrics on the number of times the firewall was hit have become less relevant as organizations move to layered controls and zero trust.

“ When relaying information to the board, be sure to convey ‘how they should feel.’ Should the board be happy or worried? What do you expect the board to do with the information—be informed, question it, or take action? Make sure they understand both the what and the why of what you are sharing. ”

Michael Johnson
CISO, Meta Financial Technologies
Meta Platforms



Examples of Metrics

- **Phishing**
 - Click rate or reporting rate
- **Controls Coverage**
 - Percentage of systems consistent with policy for a particular control
 - Controls may include patching, MFA, WAF, encryption, EDR, etc.
- **Scan Findings**
 - Percentage of critical scan findings that are open longer than the service-level timeframe
- **Incidents**
 - Number of severe incidents the company had since the last update
- **Application Security**
 - Percentage of critical applications that undergo security testing

This is an excerpt of the examples we found in our research. For the full list of all metrics, see [page 27](#).

Reporting on Significant Incidents

The board materials in our sample all cover significant cybersecurity incidents that have affected the company.

Discussions on incidents cover issues such as:

- Number of incidents by severity
- What happened in the incident
- What is known about the attacker
- How prepared the company was
- Analysis of root causes
- Metrics on response time
- How the company responded
- How successfully incidents were managed
- The type of impact on the business

In some companies, incidents discussed with the board include:

- Incidents experienced by third parties
- Natural disasters, including the COVID-19 pandemic
- Lost business due to inability to meet customer security requirements
- The discovery of a major vulnerability such as Log4j



EXAMPLE DIAGRAM

Incidents by Business Impact – [Page 24](#)

“I’m always interested in the different ways that CISOs update their board. Some of the differences are industry-based, some board makeup, maturity of the program, or how CISOs individually present.”

Gary Harbison
Global CISO, Bayer



Providing Updates on Security Initiatives

The CISOs in our research typically update the board on key security initiatives. Examples of initiatives include:

- An initiative responding to a supply chain incident, focused on securing all elements involved in developing, authenticating, and signing of the company's software products
- Efforts made over the past five years to improve resiliency against ransomware

The following types of information may be included for high-priority initiatives:

- Qualitative descriptions of progress or accomplishments
- Metrics and their targets, e.g., "Requirement: 100% of assets registered. Results to date: 95% of assets registered."
- The reasoning behind specific initiatives and/or their roadmap, e.g., a brief explanation of zero trust principles



EXAMPLE CHARTS & DIAGRAMS:

Security Initiatives: Capabilities Before and After – [Page 25](#)

Security Initiatives: Status of Key Initiatives – [Page 26](#)

“ It's important to develop a deep level of trust with your board. When you are giving any numbers or data or detail, make sure it is on a very strong foundation because you will be held accountable. And when you commit to a date, make sure you deliver. ”

Vishal Salvi
Global CISO & Head of
Cyber Security Practice, Infosys



Conclusion

Although there are common threads in the topics included in board updates, the level of emphasis given to different topics varies widely. For instance, some have a metrics dashboard as the centerpiece, while others focus on narratives and use metrics sparingly.

Our research found that differences in emphasis corresponded with differences in how CISOs view their accountability to the board, framed in terms of *metrics*, *roadmap*, or *risk reduction*, or a combination of the three:

- **Metrics frame:** Updates include a set of metrics in a dashboard which is used to show continuous improvement. The CISO is accountable for progress towards targets for those metrics.
- **Roadmap frame:** Updates focus on discussing the security roadmap and progress on its implementation. The CISO is accountable for delivering against the roadmap.
- **Risk reduction frame:** A significant part of the update is devoted to magnitudes of specific risks. The CISO is accountable for maintaining a prioritized list of risks and showing how these risks are being reduced.

In addition to differences in emphasis, there was wide variation in the content. CISOs and boards have a wide range of views on what approach is most effective and what content is most interesting.

“I think most of us, even those who have been giving updates to boards for a while, are always on the lookout for new ideas on how to communicate better with our boards.”

Richard Hale
Global CISO,
Sony Group Corporation



Appendix I: Examples of Tables of Contents for Board Updates

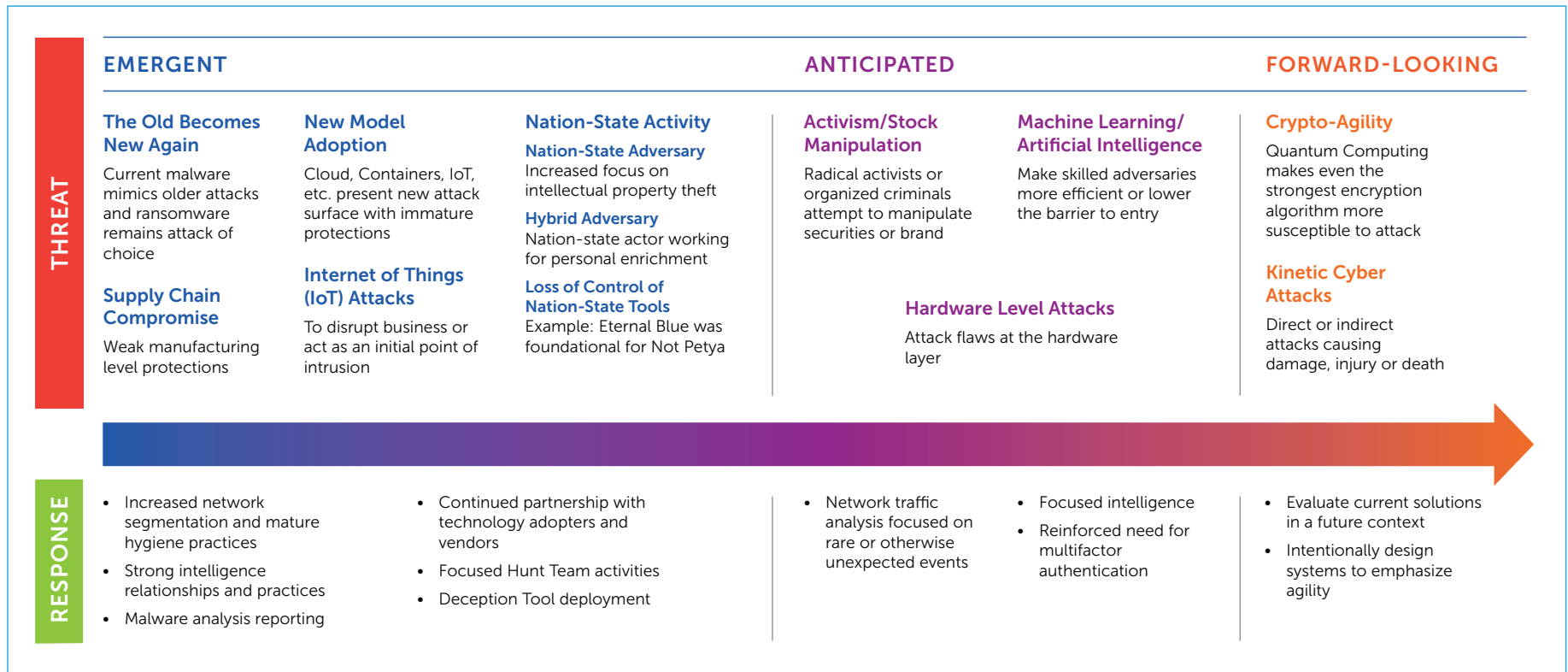
The following table shows examples of tables of contents from eight board updates.

Example 1	Example 2	Example 3	Example 4
<ul style="list-style-type: none"> • Threat Landscape • Security Status • Risk Coverage and Shadow IT • Incidents & Root Causes • Current Residual Risk and Key Risk Indicators • Cyber Culture and Trust • Cyber Strategy 	<ul style="list-style-type: none"> • Written reports every quarter: <ul style="list-style-type: none"> – Metrics – Risk register – CMMC • Security governance initiative • Cybersecurity strategy (1x per year) • Recruiting and people (1x per year) • Special topics (2x per year), e.g., <ul style="list-style-type: none"> – Operation Shields Up – Threat landscape/risk profile – CMMC 2.0 – Pen test 	<ul style="list-style-type: none"> • InfoSec Statistics • Program Capability and Maturity Assessment • External and Internal Testing of InfoSec Controls • Key Program Risks • Threat Landscape • Events and Response Time • Security initiatives • Vulnerability Trending and Market Risk Scorecard • Special topics as requested <ul style="list-style-type: none"> – Tabletop every significant industry cyber event 	<ul style="list-style-type: none"> • Threat and Regulatory Landscape • Results from independent assessments • Strategy and program • Risk register/risk management • Security incidents • Key Performance Factors
Example 5	Example 6	Example 7	Example 8
<ul style="list-style-type: none"> • Insights on programs and priorities <ul style="list-style-type: none"> – Previous year’s programs and new programs • Secure Development Lifecycle: Security Assessments & Risk Mitigation • Customer engagement <ul style="list-style-type: none"> – Responding to questions about security, privacy, and trust posture • Incident Command: Incidents of Note • Appendix: Secure Development Lifecycle Red Status 	<ul style="list-style-type: none"> • Summary upfront <ul style="list-style-type: none"> – Objective, key action required • Assessment of overall risk profile • Security oversight: auditors, regulators, and customer • Security takeaways and initiatives focused on risks <ul style="list-style-type: none"> – Current status – Effectiveness and maturity of capabilities – Security team performance and maturity • Overview of significant events • Outlook on emerging trends and threats 	<ul style="list-style-type: none"> • Executive Summary • An overview of cybersecurity issues making headlines • Board metrics • Update on our priorities • Update on our roadmap (1x per year) • An overview of a focused area • External guest speaker (1x or 2x per year) • Tabletop exercise (1x per year) 	<ul style="list-style-type: none"> • Where we are tracking against our multi-year roadmap (every other quarter) • Key external engagements/metrics with customers and regulators (every other quarter) • Key personnel changes (as needed) • Significant incidents • Progress against key annual initiatives (every other quarter) • Preview of next FY priority initiatives (annually) • Contextualize Widely-Reported External Issues (as needed) • Strategic Initiatives (as needed— approx. every other quarter)






Appendix II: Examples of Charts and Diagrams

The following are examples of charts and diagrams from the board updates covered in this research.

EXAMPLE CHART – Emerging/Future Threats Mapped to Plans for Controls

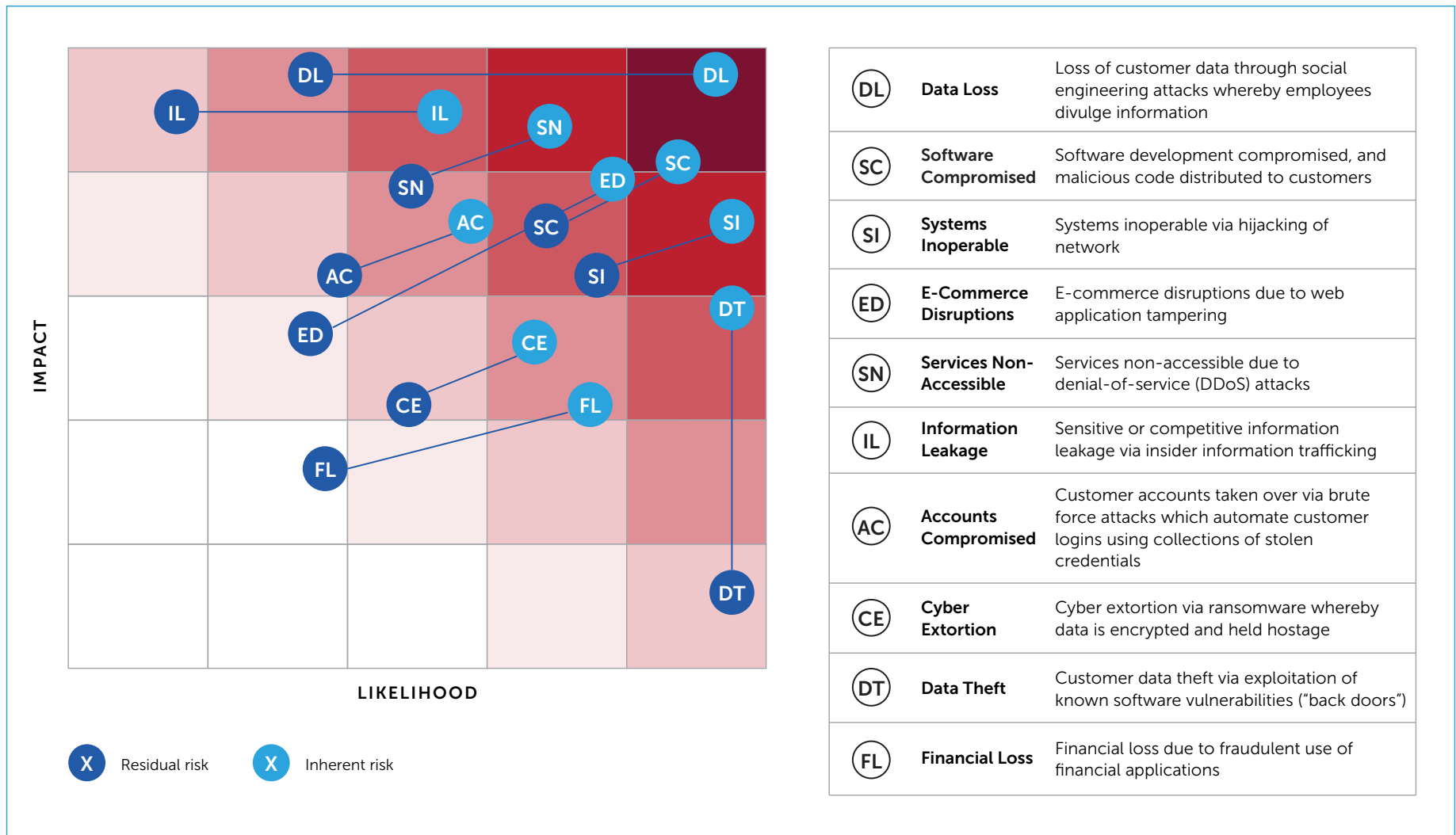


EXAMPLE CHART – Cyber Risk Management: Top 5 Risks and Countermeasures

HIGHLIGHTED ENTERPRISE RISKS	TREND v PQ	RISK COUNTERMEASURE EFFECTIVENESS
<p>Cyber resiliency readiness D P O R</p> <p>Risk of cyber incident causing prolonged outage of critical business operation due to cyber event impacting the company or a critical third party</p>		<ul style="list-style-type: none"> • Current ability to control is X + Strong layered cyber controls implemented or being deployed – Gap in tabletops executed
<p>Cyber controls effectiveness D R</p> <p>Loss or exposure of sensitive data due to gaps in cyber controls on critical business processes</p>		<ul style="list-style-type: none"> • Current ability to control is X + Strong layered cyber controls implemented, strong strategy for future segmentation – Gaps in visibility exist + Cyber Maturity metrics on target
<p>Cyber M&A coverage and efficiency P O</p> <p>Lack of strong playbooks for acquisitions leads to slow and costly integrations with larger risk of post acquisition breach impacting brand and financials</p>		<ul style="list-style-type: none"> • Current ability to control is X + Pre-due diligence checklists and strong security rigor – Over-reliance on operational teams to support integration – Weaker risk governance of non-integrated entities/subs leads to gaps in security controls
<p>Cyber agility and engagement P O</p> <p>Failure to modernize cyber approach in alignment with technology modernization leads to slowdown of digital transformation efforts and inhibits business innovation</p>		<ul style="list-style-type: none"> • Current ability to control is X + New leadership team making active investments in process improvements and enhancements – Core processes inconsistent in execution, significant backlog
<p>Cyber attrition and culture O</p> <p>Inability to sustain critical cyber operations leading to breach or regulatory incident due to high attrition of key cyber talent</p>		<ul style="list-style-type: none"> • Current ability to control is X + New leadership team making active investments in process improvements and enhancements – Core processes inconsistent in execution, significant backlog
<p>RISK CATEGORIES: Data Loss Product Related Operational Regulatory</p>		

EXAMPLE CHART – Heatmap: Top Cyber Risks with Inherent vs. Residual Risk

The difference between inherent and residual risk is the reduction in risk brought about by controls.



EXAMPLE CHART – Market Risk Scorecard: Status of Controls in Each Country

	Country A	Country B	Country C	Country D	Country E	Country F	Country G	Country H	Country I	Country J	Country K	Country L	Country M	Country N
1 Risk Assessment and Treatment														
2 Security Policy								X						
3 Organization of Info Security									X					
4 Asset Management	X	X	X	X	X	X	X	X	X	X	X	X	X	X
5 Human Resources Security														
6 Physical/Environmental Security														
7 Communications/Operations Mgt				X			X			X		X		
8 Access Control							X			X		X		
9 IS Acquisition, Dev, & Maintenance						X	X	X		X		X	X	X
10 IS Incident Management														
11 Business Continuity Management	X	X	X		X	X	X		X		X	X	X	X
12 Compliance														

X Indicates a domain score below 80%
 Indicates a domain score above 80%

EXAMPLE DIAGRAM: Security Posture: Product Risks by Business Unit

For each business unit, the number of applications is indicated as green, yellow, and red for risk posture and for progress on plan. An appendix gives an action plan for each product indicated red.

Leader	Risk Posture			Progress on Plan			# of Clouds
Business Unit Leader One	18	11	0	22	7	0	29
Business Unit Leader Two	10	7	1	18	0	0	18
Business Unit Leader Three	3	1	1	3	2	0	5
TOTALS	31	19	2	43	9	0	49

From the Appendix:

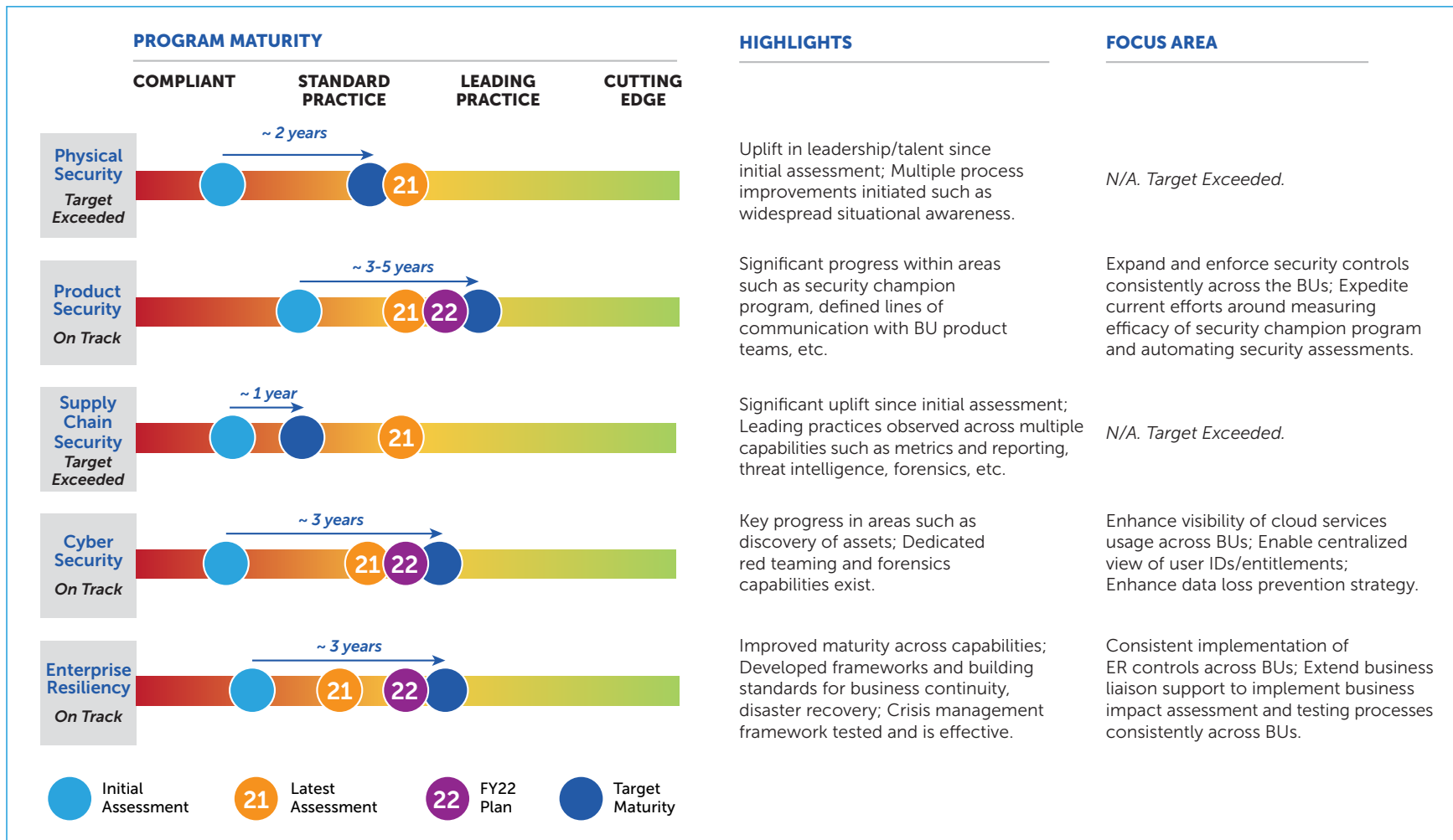
Product X: Risk Posture is Red
 (Names of the Engineering Lead(s), Business Unit Lead, GM, Security Lead, and Engineering Team Security Lead)

To move from RED to YELLOW status, the Engineering Team needs to address key security gaps. The team is engaged in remediation with the security organization. The most urgent of these are:

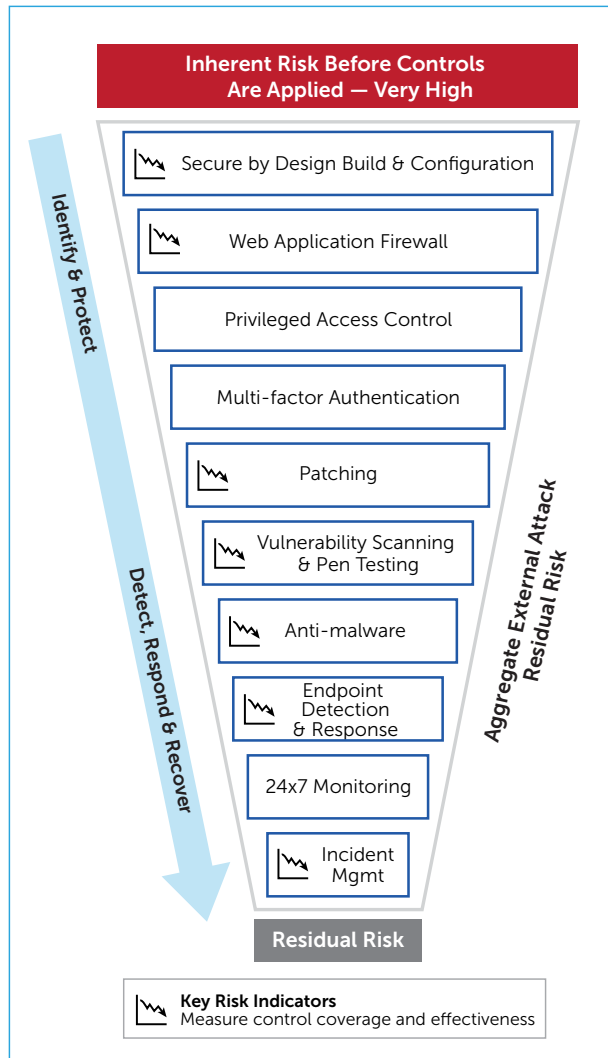
- Key Security Gap #1 – description of gap and remediation elements
- Key Security Gap #2 – description of gap and remediation elements
- (List as many as are required to move the status to YELLOW)

Good Security Risk Posture/Progress on Plan
 Some Risk in Security Risk Posture/Progress on Plan
 Significant Risk in Security Risk Posture/Progress on Plan

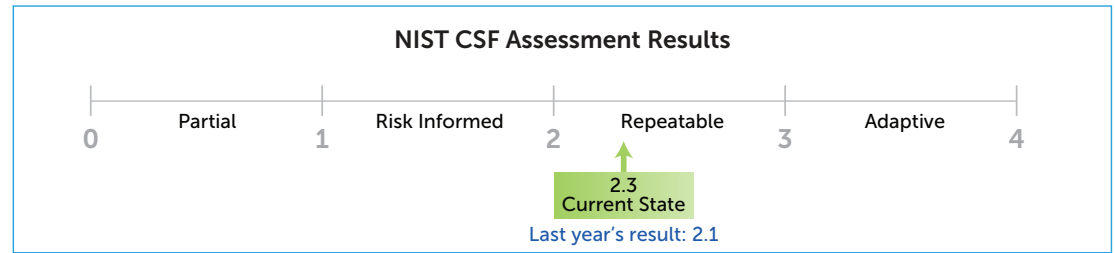
EXAMPLE CHART – Security Transformation Roadmap: Status of Program Maturity



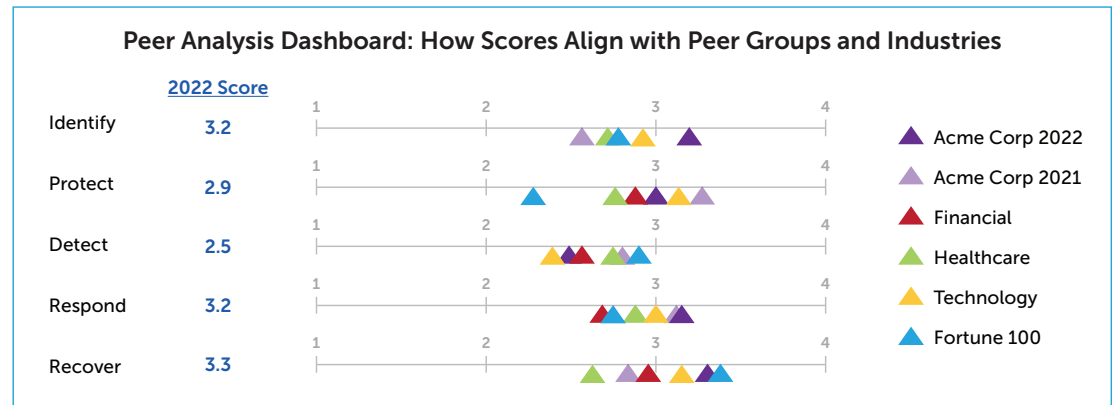
EXAMPLE DIAGRAM – Risk Mitigation: Inherent Risks Reduced Through Layered Controls



EXAMPLE DIAGRAM – Current State of Maturity



EXAMPLE CHART – Comparison of Maturity Scores with Peers

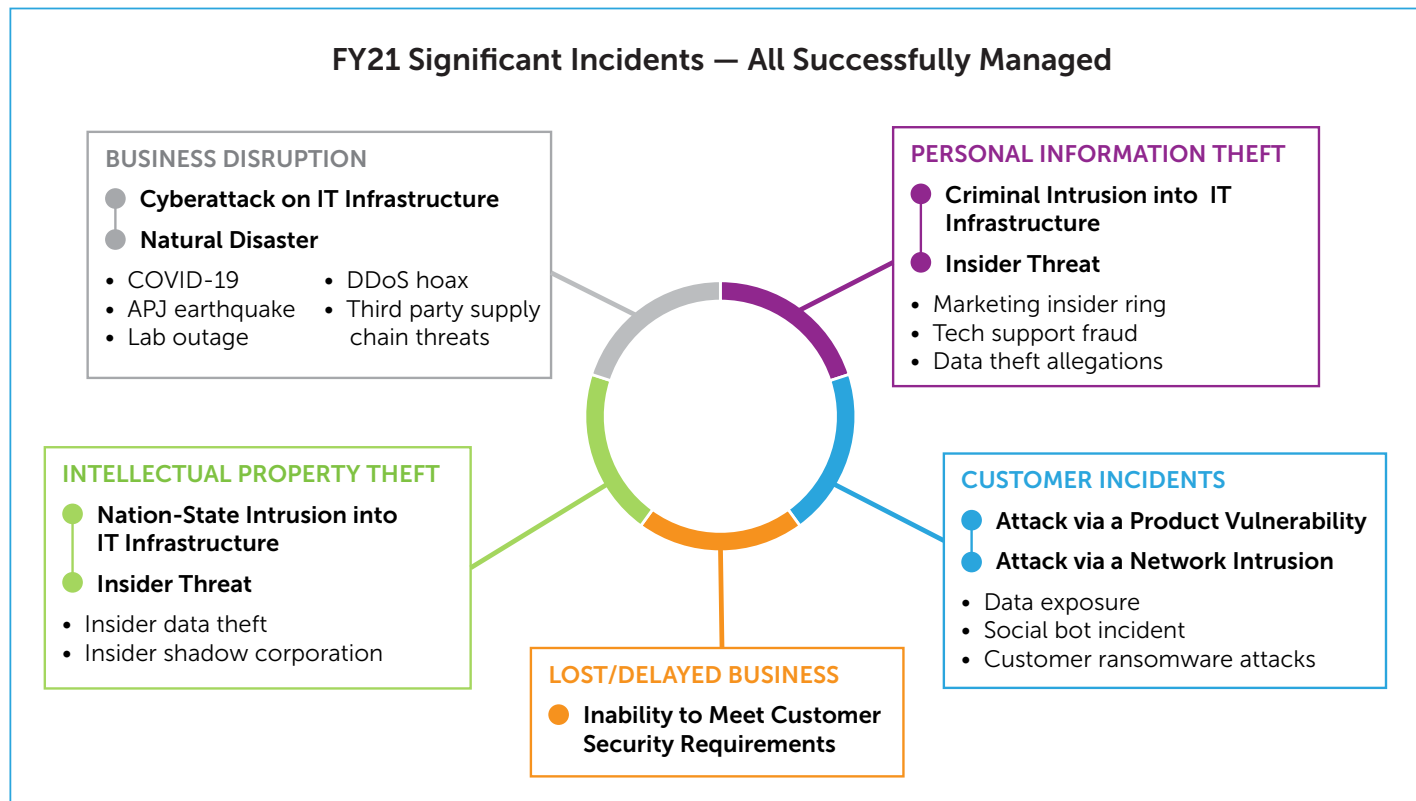


EXAMPLE CHART – Maturity Score Chart: Current vs. Target Maturity Scores for Security Objectives







OBJECTIVE	PROGRESS				CURRENT STATE	TARGET STATE
	TIER 1	TIER 2	TIER 3	TIER 4		
Technology and Information Best Practices		●	○	○	Lorem Ipsum	Lorem Ipsum
Embrace Modernization	●	○		○	Lorem Ipsum	Lorem Ipsum
Comprehensive Asset Inventory		●	○	○	Lorem Ipsum	Lorem Ipsum
Enterprise Information Management		●	○	○	Lorem Ipsum	Lorem Ipsum
Enterprise Architecture		●	○	○	Lorem Ipsum	Lorem Ipsum
Vulnerability Management		●	○	○	Lorem Ipsum	Lorem Ipsum
Cyber Shared Services		●	○	○	Lorem Ipsum	Lorem Ipsum

● = Current State
 ○ = Year End 2021
 ○ = Target State
 | = Industry Peers

EXAMPLE DIAGRAM – Incidents by Business Impact



EXAMPLE CHART – Security Initiatives: Capabilities Before and After

FOCUS AREA	BEFORE	→	AFTER	DETAILS
User Access 	Single Factor Login		2-Step Verification	<ul style="list-style-type: none"> Completed corporate associate deployment Integration for store associates
Payment Card Data 	X X X X X X		X X X X X X	<ul style="list-style-type: none"> X x x x x x
Store Level Security 	X X X X X X		X X X X X X	<ul style="list-style-type: none"> X x x x x x
Threat Detection 	Passive Monitoring		Hunt Capabilities	<ul style="list-style-type: none"> Recruited talent, built capability and deployed deception technologies
Breach Impact 	X X X X X X		X X X X X X	<ul style="list-style-type: none"> X x x x x x
Attack Surface 	X X X X X X		X X X X X X	<ul style="list-style-type: none"> X x x x x x

EXAMPLE CHART – Security Initiatives: Status of Key Initiatives

PROGRAM	BUSINESS RISK AREAS	FY22 KEY INITIATIVES
Physical Security	BD PI IP	<ul style="list-style-type: none"> Enhance Travel Risk Management program using lessons learned from pandemic response Optimize Fusion Center through team and facility consolidation
Product and Application Security	CI LB	<ul style="list-style-type: none"> Expand and improve management of open source and third-party components in products & applications Expand the crowdsourced testing program Drive adoption and scale of Secure Development Lifecycle through automation and self-service tooling Drive Secure Development Lifecycle practices to a standard maturity level in actively developed products Integration of Secure Development Lifecycle in supply chain management for all types of suppliers
Supply Chain Security	BD CI LB	<ul style="list-style-type: none"> Enhance Cybersecurity of Manufacturing environments Expand implementation reach of Supply Chain Standards (inventory controls, reverse logistics, etc.)
Enterprise Resiliency	BD LB	<ul style="list-style-type: none"> Operationalize the Resiliency Management Technology Platform Implement a new global Disaster Recovery Governance framework
Cybersecurity	PI CI LB IP	<ul style="list-style-type: none"> Drive Network Security technology refresh to replace aging cyber equipment Improve Security Visibility at strategic corporate access points Automate Security Incident Response functions to enable analysts to focus on higher value tasks Improve enterprise ransomware resiliency preparedness Extend vulnerability management capabilities in prioritized environment
Risk Key BD Business Disruption PI Personal Information CI Customer Incidents LB Lost Business IP Intellectual Property		Cross-Program <ul style="list-style-type: none"> Align Security Team strategy to proactively address the changes in risk posture created by the NewOffer strategy Lead definition and specification of NewOffer security strategy Significantly expand Insider Risk Management program

Appendix III: Metrics Included in Board Updates

This chart contains the full list of metrics amalgamated from the board updates covered in this research.

Category	Example
Application security	Number of products with good security risk posture/some risk/significant risk
	% of applications that undergo static and dynamic security testing
Audit	% of audit findings that remained open for more than X days
	Control failure rate for most recent SOX audit/PCI audit
Customer trust	% of customer checklists completed within target timeframe
	% of addressable requests satisfied with industry standard documentation
	# of customer security requests
	# of unique visitors to the customer trust portal
	# of downloads from customer trust portal
Hygiene	Phishing click rate
	Phishing reporting rate
	% of endpoints with control X
	% of critical systems consistent with policy for control X (where X could be MFA, WAF, encryption, etc.)
	# of Critical and High vulnerabilities remediated within 30 days
	% of public cloud assets that are fully protected
	% of websites behind a correctly configured WAF
	% of assets registered
	% of assets that have undergone vulnerability scanning
	% of critical scan findings that were open longer than the service-level timeframe

Category	Example
Incidents/ Preparedness	# of (severe) incidents
	# of tabletop exercises completed
	Average time to detect/respond/mitigate/contain after an event
	% of action items from readiness plans that were completed
Security governance	Percentage of company zones that: <ul style="list-style-type: none"> • Are not under security governance • Do not have a signed-off plan for meeting security requirements • Are not on track for meeting the milestones in their security plan
	Dollar value of company zones that: <ul style="list-style-type: none"> • Are not under security governance • Do not have a signed-off plan for meeting security requirements • Are not on track for meeting the milestones in their security plan
Service to the business	% of key security workflows meeting service level objectives
Talent	Employee turnover rate
Third-Party risk	% of suppliers whose risks are managed
	Third party performance against Service Level Objectives (measured on a scale from 1-10)

Appendix IV: Examples of Metrics Dashboards

Some CISOs in our research included a metrics dashboard in their update to the board. Here are three examples.

Example 1 of a Metrics Dashboard

Security Baseline: X				
Industry-Specific Controls	Industry-specific metric x%		Industry-specific narrative 1	
	Industry-specific metric x%		Industry-specific narrative 2	
Metric		How Measured		Progress Against Targets
IT Controls	Patching x % for Windows, Linux/Unix, Citrix		% of systems in scope which meet agreed patching frequency	Trend of Patching
	IT Hardening	x%	% of compliant assets (x) within in-scope assets (x) which meet agreed targets	Trend of IT Hardening – Open deviations reduced by x from x – Forecasting x deviations will be cleared by x
	Cloud Hardening	x% x%	x public cloud 1 assets, of which x are fully compliant. x public cloud 2 assets, of which are fully compliant.	Trend of Cloud Hardening
	Anti-Malware Tools Email Gateway Hygiene	x x%	x assets covered across estate x active email domains across x business units	Trend of Anti-Malware Deployment
Security Tooling	Endpoint Detection & Response (EDR) Coverage	Tool 1 x% Tool 2 x%	Tool 1 software agents are deployed across x assets. (Compatibility for deployment of Tool 1 and Tool 2 agents is x% and y% respectively)	
	Web Application Firewall (WAF) Coverage	x%	% of websites behind a WAF with correct rules in blocking: x secured assets/x live assets	Trend of WAF Coverage – Coverage up x% year-over-year
Operational Metrics	Phishing Results	Non-click rate x%	Data based on year-to-date email phishing campaigns. x emails delivered across x locations. x users clicked on phishing tests from x test mails x%).	
	Security Incidents	x per month	Monthly incidents by severity	
	Vulnerabilities	x	Critical vulns open > x time period	Trend of Vulnerabilities – Number reducing with targeted actions

NOTES: • Key Risk Indicators (KRIs) shown in red under threshold, amber within range, green above threshold
• Target thresholds for KRIs shown in % are x % unless indicated

Example 2 of a Metrics Dashboard

Category	Output Metrics	Metric	Go-to-Green Plan
Third Party Relationships	% of third parties whose risks are managed	x%	<ul style="list-style-type: none"> Metrics not on-target for the quarter are shown in yellow, and the rest in green A separate sheet for each metric explains how the metric is calculated and specific goals by quarter. For each metric not on target, this column contains short statements explaining the improvement plan.
Critical Systems	% of critical systems protected according to policy	<ul style="list-style-type: none"> Security control 1: x% Security control 2: x% Security control 3: x% Security control 4: x% Security control 5: x% 	
Security by Design and Product	% of applications that undergo static and dynamic security testing	x%	
Compliance	% of open findings that were closed within the target timeframe	x%	
People, Culture, and Resources	Phishing click rate	x%	
	Employee turnover rate	x%	
Incident, Threat Readiness, and Business Resiliency	% of action items from readiness plans that were completed	x%	
	Number of Tabletop exercises completed	x	
Program Maturity	Maturity score	x Industry average: x	
	Output of assessments and status of remediations	<ul style="list-style-type: none"> Bullets 	

Example 3 of a Metrics Dashboard

Category	Metric	How Measured	Target Score	August Score
Cyber Compliance	Supplier compliance	Performance against SLO	x	X
	Customer compliance checklist response rate	Percent of checklists completed	=> x % response based on 3-month moving average	x%
Cyber Maturity	Phishing clicks	Click rate average for last campaign	< x %	x%
	Patching quality	Weighted percent of patching completed of Critical & High vulnerabilities within target SLO	> x % SLO met	x%
	Maturity model	Maturity model score	x	x
Cyber Operations	Mean time	Time from when event occurred to when event confirmed	x days, x hrs, x min	x days, x hrs, x min
	Operational SLAs	SLO performance for x security workflows	x	x

Previous Months' Metrics	June Score	July Score
Supplier compliance	X	X
Customer compliance checklist response rate	x%	x%
Phishing clicks	x%	x%
Patching quality	x%	x%
Maturity model	x	x
Mean time	x days, x hrs, x min	x days, x hrs, x min
Operational SLAs	x	x

NOTES:

SLO = Service Level Objective

SLA = Service Level Agreement.

If targets not met, scores would be flagged red 🚩 or yellow 🟡

Appendix V: RSAC ESAF 2022 Program Committee Biographies



Justin Acquaro

Chief Information Security Officer
Evernorth (Cigna Corporation)

Justin leads Evernorth's cyber security organization, which is responsible for securing health care outcomes for millions of patients leveraging the four lines of business: Pharmacy, Benefits Management, Care+ and Intelligence. Previously at GE, he was Global Chief Information & Product Cyber Officer and spent 10 years in various senior leadership positions. Justin is a seasoned security leader with 18+ years of his career helping large companies, including Sprint, Booz Allen Hamilton, and GE, build robust and sustainable security programs.



Brad Arkin

Senior Vice President, Chief Security and Trust Officer
Cisco

Brad leads Cisco's Security and Trust Organization, whose core mission is to ensure Cisco meets its security and privacy obligations to customers, regulators, employees, and other stakeholders. Previously he was Chief Security Officer at Adobe and has held management positions at @Stake and Cigital. He holds a B.S. in computer science and mathematics from the College of William and Mary, M.S. in computer science from GWU, and MBA from Columbia University and London Business School.



Jason Barnett

Vice President, Chief Information Security Officer
HCA Healthcare

Jason leads nearly 100 security professionals across all aspects of information security including threat and vulnerability management, security architecture, vendor security risk management, controls assurance, regulatory compliance, eDiscovery, and digital forensics. Previously, he built a very successful security consultancy highly focused on remediation of healthcare regulatory compliance findings and driving the establishment of cyber resilience across several industries, including healthcare, financial, logistics, distribution, and advertising. Jason graduated from Murray State University.



Chris Betz

Chief Information Security Officer
Capital One

Chris joined Capital One in April 2020 as the Chief Information Security Officer, where he leads cybersecurity across the Enterprise. Previously, he served as CSO at CenturyLink and held security roles at Apple, Microsoft, CBS Corporation and the National Security Agency (NSA).

RSAC ESAF 2022 Program Committee Biographies



Jerry R. Geisler III

Senior Vice President and Chief Information Security Officer

Walmart

Jerry leads Walmart's global information security department. His responsibilities encompass data security not only for Walmart's 230 million customers but also its 2.3 million associates. He oversees information security strategy, engineering, operations, services, testing and assessment, risk, governance, and compliance for the global enterprise. Under Jerry's leadership, Walmart's information security program is considered as a forward-thinking industry leader focused on emerging best-in-class information security practices, innovation, and business enablement broadly engaged across IT, ICS, cloud, platform, and product security domains.



Richard A. Hale

Global Chief Information Security Officer

Sony Group Corporation

Richard currently leads Sony's global information security effort. Previously he had various cybersecurity jobs in the U.S. Government, finishing as the Department of Defense CISO. While in the government, Richard helped develop some of the foundational cybersecurity approaches within government that have become global industry best practices.



Gary Harbison

Global Chief Information Security Officer

Bayer

Gary leads the Cyber Security Risk Management (CSRM) organization at Bayer with global ownership of cybersecurity, IT risk management, and protection of Bayer's critical data. Gary and CSRM are focused on managing Bayer's risks and cyber threats globally and enabling the business with pragmatic security solutions. Gary has 25 years of overall IT experience, mostly focused within the cybersecurity domain, including with multiple global Fortune 500 companies, as well as public sector experience with the US Department of Defense.



Katie Jenkins

Executive Vice President for Global Cybersecurity and Chief Information Security Officer

Liberty Mutual Insurance

Katie is responsible for the global cybersecurity program, ensuring protection of company data, defense of the brand and minimizing business impact of cyberattacks. She leads enterprise cybersecurity policy, strategy and programs. Prior to this role, Katie was Vice President and Senior Director, leading cloud and security enablement programs for Liberty's commercial insurance division. Her previous information security experience includes positions with AT&T Consulting Solutions, VeriSign, Guardent and PWC. Katie serves as a board member of the Advanced Cyber Security Center.

RSAC ESAF 2022 Program Committee Biographies



Michael Johnson

Chief Information Security Officer,
Meta Financial Technologies
Meta Platforms, Inc.

Michael oversees security for all of Meta's payments and financial services. Previously Michael served as Capital One's CISO and Senior Vice President, leading and managing information security, cybersecurity operations, and security technology innovation. Prior to joining Capital One, Michael served as the Chief Information Officer (CIO) for the U.S. Department of Energy, and in other key cyber-focused executive roles in the U.S. Government at the Office of the Director of National Intelligence, the U.S. Department of Homeland Security, and the White House Executive Office of the President.



Robert Martin

Chief Information Security Officer
Alberta Health Services (AHS)

Robert is responsible for all aspects of the information and cybersecurity program for AHS, the largest healthcare delivery organization in Canada, with over 120,000 staff, physicians, and volunteers. He is co-chair of the Enterprise Risk Management Executive Committee and leads security operations, policy, governance, compliance, architecture, awareness, and service management teams, with a focus on identifying and managing risk. Previously, Robert was a trusted advisor and consultant in information security and risk management for large public and private sector clients.



Catherine McCully

Chief Information Security Officer
Procter & Gamble

Catherine leads cybersecurity and information security across the organization. She is responsible for the strategies and execution to ensure confidentiality, integrity, and availability of P&G's vast environment. Previously, Catherine held cybersecurity and information security related roles in global financial services and retail Fortune 100 companies. In these roles, her experience ranged from engineering and risk management to front line Incident Response and key leadership. Catherine has led transformative changes across people, processes, and technologies.



Michael McNeil

Senior Vice President, Global Chief
Information Security Officer
McKesson

Michael is responsible for enhancing and overseeing McKesson's information and operational technology security strategy program and managing information security governance. Previously he was Global Product Security and Services Officer for Royal Philips and held senior leadership positions at Medtronic, Liberty Mutual Group, Pitney Bowes, and Reynolds & Reynolds. He holds several board and executive member positions, including the Healthcare and Public Health Sector Coordinating Council (HSCC) Executive Committee and the Health Information Sharing and Analysis Center (H-ISAC).

RSAC ESAF 2022 Program Committee Biographies



Vishal Salvi

Global Chief Information Security Officer & Head of Cyber Security Practice

Infosys

With rapid changes shaping the digital enterprise, Vishal seeks to amplify conversations around advances and innovations in cybersecurity and enhancing cyber resilience. Previously, Vishal was an Advisory Partner, Cyber Security at PwC, SVP & CISO at HDFC Bank, SVP & Head of Cyber Ops at Standard Chartered Bank; and held IT roles at Global Trust Bank, Development Credit Bank, and Crompton Greaves. Currently, he is an Independent Director at Data Security Council of India and serves on various advisory committees.



Emma Smith

Chief Information Security Officer
Vodafone

Emma leads cybersecurity globally at Vodafone, alongside Technology Strategy and Assurance. The cybersecurity team sets risk appetite and policy, manages security risk, defines security architecture, delivers and operates security tools and runs global 24/7 cyber defence capabilities. Emma is passionate about security, and an active sponsor for diversity and inclusion in the workplace. She also holds an independent Security Advisor role for a large Retail company. Previously, Emma was CSO at RBS/ NatWest, leading an integrated security team.



JR Williamson

Senior Vice President and Chief Information Security Officer

Leidos

JR is accountable for information security strategy, business enablement, governance, risk, cybersecurity operations, and classified IT at Leidos. He is a CISSP, Six Sigma Black Belt, and serves on the Microsoft CSO Council, the Security 50, Gartner Advisory Board, the Executive Security Action Forum Program Committee, DIB Sector Coordinating Council, WashingtonExec CISOs, Evanta CISO Council, the National Security Agency Enduring Security Framework team, and is the Chairman of the Board of the Internet Security Alliance.