CISOs in the Boardroom

Presenting Cyber Risk Storyboards with Confidence

Presented by Clemence Beinse, Senior Consultant & Nichol Deaddis, Solutions Director at Galvanize, a Diligent Brand
Today’s Presentation

1. Putting Cyber Security Back on the Map
2. Aligning Cyber Security Metrics
3. Defining Meaningful Metrics
4. Managing the Business of Cyber Security Risk
5. Reporting Confidently with Storyboards in HighBond
Putting Cyber Security Back on the Map
Data breaches, ransomware attacks and concerns over risks tied to the global pandemic have heightened interest in cybersecurity among corporate boards of directors.

BoDs have become more engaged in security matters, have a keener understanding of cyber issues, and have begun asking more sophisticated questions about risk exposure and ways to manage it.

https://www.csoonline.com/ - Dec 2020

CSO serves enterprise security decision-makers and users with the critical information they need to stay ahead of evolving threats and defend against criminal cyberattacks.
Governments and businesses have struggled to address compounding repercussions in the form of workforce challenges, disruptions in essential supplies and social instability.

They have had to balance health security imperatives against the economic fallout and rising societal anxieties, while relying on digital infrastructure in unprecedented ways.

Cyber Attacks on the Rise

New working patterns may increase cyberattacks and data fraud.

The techno-optimism that accompanied the rise of the internet was already dampened by rising cybercrime, concerns about the security of networked technologies, the risk of cyberwar and suspicions about data manipulation to shape perceptions.
Keys to Alignment

Implement **governance structures** that are fit for purpose — develop a set of key performance indicators and key risk indicators that can be used to communicate a risk-centric view in executive and board reporting.

Focus on **Board engagement** — communicate in a language the board can understand; consider a risk quantification program to more effectively communicate cyber risks.

Source: EY Global Information Security Survey 2020
How does security evolve from bolted on to built-in? Bridging the relationship gap to build a business aligned security program.
Metrics – It’s all about how you look at it
Aligning on the Right Metrics

Board & Executive Management
External Focused Metrics:
• Delivering on Vision & Mission
• Customer & Stakeholder Value

CISO & Security Teams:
Internally Focused Metrics:
• Security Domains (Access Mgt, SecOps, Sec Architecture)
• Compliance with Regulations & Audits Requirements

Source: EY Global Information Security Survey 2020
How does security evolve from bolted on to built-in? Bridging the relationship gap to build a business aligned security program.
Bridging the Gap

✓ Use KPIs/KRI, not detailed data

✓ Derive metrics from the same underlying data set

✓ Transform the data, quantify & add Business Context
Cybersecurity Metrics
Defining Meaningful Metrics

Organize Metrics by Security Domain or Department
- Governance
- Identify & Access Mgt
- Security Operations
- Security Architecture

Select Metrics that Influence Behavior
- Promotes data & risk-based decisions
- Drives action
- Avoid “So What?” metrics

Establish Baselines & Targets
- Comparison of future performance
- Quantify metrics in business terms ($, %)
## Examples of Key Metrics

<table>
<thead>
<tr>
<th>Area</th>
<th>Metrics</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance &amp; Compliance</td>
<td>Time from hire date to Security Awareness Training Completion date</td>
<td>HR System, Training System</td>
</tr>
<tr>
<td></td>
<td>Number of active acceptances, by department</td>
<td>GRC</td>
</tr>
<tr>
<td></td>
<td>Number of active exceptions, by owner, by age in months</td>
<td>GRC</td>
</tr>
<tr>
<td></td>
<td>Critical systems where identified control gaps have not been remediated</td>
<td>GRC</td>
</tr>
<tr>
<td></td>
<td>Trends of gaps identified though self-assessment process compared to audit findings</td>
<td>GRC</td>
</tr>
<tr>
<td>Identity Management</td>
<td>Time from termination to Access Revoked for terminated employees (in hours, by term)</td>
<td>HR system (term date), IDM (access revoked date/time)</td>
</tr>
<tr>
<td></td>
<td>Access not re-certified/expired (count, by department, over last 12 months)</td>
<td>IDM</td>
</tr>
<tr>
<td></td>
<td>Accounts within critical systems whose privileges have not been reviewed and approved</td>
<td>IDM</td>
</tr>
<tr>
<td></td>
<td>Inactive (terminated / dormant / transfer) user accounts that have not been disabled</td>
<td>HR system (term date), IDM (access revoked date/time)</td>
</tr>
<tr>
<td>Security Ops</td>
<td>Time to detection (average time in minutes, by month, over last 12 months)</td>
<td>Incident management (GRC)</td>
</tr>
<tr>
<td></td>
<td>Time from detection to containment (average time in minutes, by month)</td>
<td>Incidents management (GRC)</td>
</tr>
<tr>
<td></td>
<td>Operational time where a critical system was unavailable</td>
<td>BCM</td>
</tr>
<tr>
<td></td>
<td><strong>Critical/High Vulnerabilities Days Open (average, by month, over last 12 months)</strong></td>
<td>VMI, GRC</td>
</tr>
<tr>
<td></td>
<td>Assets (applications, hosts, etc.) with critical/High vulnerabilities (average count, by month)</td>
<td>End point systems</td>
</tr>
<tr>
<td></td>
<td>End point devices without automatic protection per policy/standards</td>
<td>Configuration management systems</td>
</tr>
<tr>
<td></td>
<td>Percentage of systems with configurations that deviate from approved standards</td>
<td>GRC, PenTest, Architecture review (manual)</td>
</tr>
<tr>
<td>Security Architecture</td>
<td><strong>Percentage of critical application/systems with and without a security review</strong></td>
<td>GRC, PenTest, Architecture review (manual)</td>
</tr>
<tr>
<td></td>
<td>Count of critical application/systems that have at least one critical/high finding, by month</td>
<td>GRC, PenTest, Architecture review (manual)</td>
</tr>
</tbody>
</table>
Beyond the Metrics
The Business of Managing Cybersecurity Risks

- Manage Business of Risk via Operational Meetings
- Use Data Driven Metrics to Track Performance
- Leverage Robotics for data mining, aggregation, analysis, & reporting
- Quantify Cyber Risk & Business Alignment via Real-Time Storyboards

Cybersecurity Risk Management
The Solution
ACL Robotics for data analytics

1. **Acquire Data**
   - Import directly from your data source and clean your data

2. **Analyze**
   - Analyze risk and uncover data insights

3. **Automate**
   - Let Robots run your analytics on a schedule and surface KPIs, KRIs and KCIs

4. **Monitor & Report**
   - Let Robots update dashboards and visualizations
ACL Robotics – 100+ Data Connectors
Analysing Data

Putting the robots to work

- Analyze 100% of your data
  *Make accurate conclusions & increase business owner visibility*

- Built-in version control for scripts
  *Collaborate effectively*

- Schedule analytics on recurring basis
  *Monitor continuously and reduce risk exposure*

- Use Machine Learning to...
  *Predict patterns & anomalies*
Vizualising Results in Storyboards

- Easily customizable storyboards
  *Save Time*

- Prepare once; continually updated
  *Drive data driven decisions*

- Share with stakeholders to Collaborate effectively
Managing the Business of Cyber Security Risk

- Define metrics that **drive behavior**
- Manage by numbers via regular “Ops” meetings & hold leaders/teams accountable
- Automate via Analytics & Robotics
- Use **Storyboards** to provide transparency to internal stakeholders
- Measure performance against baselines
- Use defendable, quantifiable metrics **aligned to business objectives**
Demonstration of Storyboards

Cybersecurity Risk Storyboard

CISO Objectives

Lines of Business have experienced challenges meeting corporate objectives for IT Risk and Compliance.

The objectives on display in this chart have shown the highest degrees of non-conformity as of this report.

Assurance

The figures on the right average the assurance scores across all active cyber risk assessments. The individual assurance scores are calculation-based values, which allow us to benchmark how well risk is mitigated and to what extent we have the right controls in place to mitigate risk.

AVERAGE OF RISK ASSURANCE ACROSS ALL CRA

77
Q&A
Thank you!

Come speak to us at the Galvanize booth in the exhibition hall if you'd like to know more about our solution!