The First 6 Months as a CISO Determines Success or Failure

Michael Coates
CEO
Altitude Networks
@_mwc
The “CISO”

Putting Security Into Perspective
Day 0 - Role of the CISO

The role of the CISO is **NOT** to single-handedly prevent all security vulnerabilities or be responsible for every security failure.
The role of the CISO is NOT to single-handedly prevent all security vulnerabilities or be responsible for every security failure.

Instead, the CISO’s role is to build systems, technology, and processes that surface risks, empower informed risk management and enables the company to mitigate risks to an acceptable level...
Day 0 - Role of the CISO

The role of the CISO is **NOT** to single-handedly prevent all security vulnerabilities or be responsible for every security failure.

Instead, the CISO’s role is to build systems, technology, and processes that surface risks, empower informed **risk management** and enables the company to **mitigate risks to an acceptable level**... while moving at the **speed of business**.
Day 1 - Risks: What Actually Matters

Modification of Threat Pyramid, Alex Stamos, BlackHat 2017
Day 1 - What Is Security at Enterprise Scale?
Don’t Act, Listen First
CISO Instinct - Immediately take action and begin “delivering value”
Day 2 - Don’t Rush to Action

**CISO Instinct** - Immediately take action and begin “delivering value”

**Contrarian CISO Advice** - Don’t. Actually do “nothing” for first 90 days. Instead Listen!
## Day 10 - CISO to Business Leaders: 5 Questions

<table>
<thead>
<tr>
<th>Category</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empathy</td>
<td>What does your org do?</td>
</tr>
<tr>
<td>History</td>
<td>Previous interactions between org &amp; security?</td>
</tr>
<tr>
<td>Perspective</td>
<td>How do you view security at the company?</td>
</tr>
<tr>
<td>Ideas</td>
<td>What areas should security investigate?</td>
</tr>
<tr>
<td>Alignment</td>
<td>Best way to stay connected &amp; updated?</td>
</tr>
</tbody>
</table>
Ask Your Security Team
Where are the “dead bodies”?
Deliverables: Strategy, Plans & Support

Easier Said Than Done
Day 60 - Five Core Deliverables from CISO

- Company Risk Tolerance
- Listening Tour
- Security Core Controls
- Compliance Requirements
- Security as Enabler

Strategy
- Operations Plan
- Resourcing
- Org Ownership
- Reporting Structure
Day 61 - The Delivery

C Suite & Board

Security Org & Company

Peer Leaders
Don’t forget Security Allies

C Suite & Board

Security Org & Company

Peer Leaders
- Internal Audit
- Legal
- BizDev
Why All Breaches are(n’t) the CISOs Fault

Establishing Security Accountability
Day 90 - Why CISOs are (often) setup to fail
Handling Security & Risk Ownership

<table>
<thead>
<tr>
<th>Authority</th>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Handling Security & Risk Ownership

<table>
<thead>
<tr>
<th>Authority</th>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Frustrated Participant</td>
</tr>
<tr>
<td>Yes</td>
<td>Helpless Scapegoat</td>
</tr>
<tr>
<td>No</td>
<td>Frustrated Participant</td>
</tr>
<tr>
<td>No</td>
<td>Helpless Scapegoat</td>
</tr>
</tbody>
</table>
Handling Security & Risk Ownership

<table>
<thead>
<tr>
<th>Authority</th>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Risk Ownership Defines Culture

- **Unchecked Ruler**
- **Empowered and Responsible**
- **Frustrated Participant**
- **Helpless Scapegoat**

<table>
<thead>
<tr>
<th>Authority</th>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Risk Ownership Defines Culture

- Unchecked Ruler
- Empowered and Responsible
- Frustrated Participant
- Helpless Scapegoat

Authority: Yes → Yes
Accountability: No → Yes
Empowered and Responsible: The How

How to Do It

- Establish culture of risk taking & ownership
- Don’t fight risky decisions - redirect with mitigation and visibility
- Gamify for leadership traction
- Eliminate IC to IC priority battles
- Track, retro, praise/adjust
- Build feedback loops for improvement

<table>
<thead>
<tr>
<th>Authority</th>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#RSAC

ALITUDE NETWORKS

RSA Conference 2020
Build Security Culture at Leadership Level

Align Authority & Accountability for Security Actions
Day 90: Security Team Building in Negative Unemployment Markets
Security Unicorns: Stop looking for them

*Reality*
Awesome teams are built with great people in well-defined roles

*CISO Anti-pattern*
Wedging multiple security disciplines into a single headcount
Amazing Teams Need Different Roles
Spending Time vs Money

Which do you have more?

Opex, Capex, Security Staff Hours
Build a Security Talent Funnel

Document & Delegate
Focus Senior Talent

Capability Matrix,
Defined Roles & Runbooks
Empower Junior Talent

Foster Future Experts
University Interns
Co-opt Programs (Year Up)
Successful Teams Require Diversity of Thought and Background
Be a CISO and a Great Leader
Bringing it all Together
Days 1 - 180: The CISO’s First Journey

Learn  
Plan  
Align Support  
Execute
Role of the CISO Revisited

The role of the CISO is NOT to single-handedly prevent all security vulnerabilities or be responsible for every security failure.

Instead, the CISO’s role is to build systems, technology, and processes that surface risks, empower informed risk management and enables the company to mitigate risks to an acceptable level... while moving at the speed of business.
The CISO is not the *Super Hero* that Prevents All Security Risks
The CISO is the Pathfinder who guides a company to responsibly embrace risk for competitive advantage.
Thank you!

Michael Coates

michael@AltitudeNetworks.com

@_MWC