What It Takes to be a CISO in 2017

Doug Copley
Deputy CISO
Sr. Security & Privacy Strategist

February 2017
IMAGINE…

You’re the CISO… Of a bank…

In Bangladesh…

On a Friday when you’re closed…

You realize 6 huge transfers are underway…

It takes 4 DAYS to halt the transfers…

By then, $81M dollars are gone…

How can you begin to explain why…how…
AGENDA

1. Expectations of a CISO
2. Mindset and Focus
3. Insights
4. Network
5. CISO Roadmap
6. Takeaways
EXPECTATIONS
CISO – THE IMPOSSIBLE JOB? OR JUST THANKLESS

<table>
<thead>
<tr>
<th>Policy definition</th>
<th>Enforcement</th>
<th>Monitoring &amp; response</th>
<th>Audit/Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Databases</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoints</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messaging &amp;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strong Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch/Router</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patch management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard drive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web SSO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>filtering</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&amp; key management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&amp; key management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic Auditing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall/Host</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus/Anti</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>spyware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall/Host</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XML gateway</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>firewall</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-spam</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Leak</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevention</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investigation &amp;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forensics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Incident</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CISO RESPONSIBILITIES IN 2007

• Install & manage firewalls
• Install & manage internet proxy server
• Install & manage endpoint anti-virus
• Install & manage intrusion detection (if you were advanced)

Required strong technical knowledge

Primary Focus:
Technical Control Implementation
CISO RESPONSIBILITIES IN 2017

- Managing information risk
- Executive business partner (enable)
- Successfully navigating the landscape (business, regulatory, threat)
- Risk-based strategy & vision
- Leadership (security, team, change)

**Primary Focus:** Enable the business while managing risk & compliance
REQUIRES ABILITY TO WORK IN UNCERTAINTY

Day 1

What Some Days Felt Like

You are here…
Arranging deck chairs…

http://www.workinginuncertainty.co.uk/
What’s on the mind of a CISO?

1. Constantly evolving and sophisticated cyber threats
2. Struggle with visibility across locations, systems and networks
3. Fear of not being able to detect that we’ve been compromised
4. Breach headlines = unemployment (scapegoat)
What’s on the mind of a CISO?

5. Do I understand business priorities and direction?

6. Security of cloud platforms and applications

7. Not being fully prepared to respond to an incident

8. Insider threats (intentional, accidental, inadvertent)

9. Finding and retaining skilled cybersecurity talent
UNDERSTANDING THE THREATS

1. Is it the people? Employees or 3rd party? Consultants or contractors?

2. Is it technical vulnerabilities? Have they always existed?

3. Is it poor technology? Is it still supported? Does it NOT meet the needs?

4. Is it culture? Do staff identify control gaps? Are they punished for it?

5. Is it executive mgmt? When were they updated last?
MANAGING CYBER RISK

Key is appropriately managing the risks
- Policies & procedures (administrative)
- Technology tools (technical)
- Control physical access (physical)

Risk/Cost decision: Do we need to:
- Prevent it from happening?
- Detect & respond when it happens?
- Would it automatically get corrected?
- Do we get cyber insurance?
WHEN THINGS GO AWRY...
NATURAL PARTNERS IN MANAGING RISK

Corporate Compliance
» Applicable regulations
» Risk of Non-Compliance

Enterprise Risk Management
» Manages all risk across the company
» Will measure information risk the same as others

Internal Audit
» Can help raise risk awareness to Board
» Can report on control effectiveness
NATURAL PARTNERS IN MANAGING RISK

Legal Affairs – advice
- Retention, litigation, legal precedents

Human Resources
- Job Descriptions
- Training

Information Technology
- Will implement technical controls

Finance
- Will help quantify risk into currency
USERS: ASSET OR LIABILITY?

**Liability**
- Aren’t aware of policies
- Careless; make mistakes
- Contract malware
- Steal company secrets
- Sabotage systems
- Falsify data
- Steal identities

**Asset**
- Help educate others
- Police their departments
- Report risky behavior
- Help improve policies
- Help remediate events
- Pilot new controls
- Suggest new processes
VENDORS: ASSET OR LIABILITY?

**Liability**
- Lack controls
- Lack oversight
- Don’t communicate well
- Bad agreements
- Aren’t compliant
- Breach your data

**Asset**
- Help educate CISO, team
- Help deploy controls faster
- Help monitor, remediate events
- Help assess risk/compliance
- Provide expertise
- Can suggest process improvements or deployment alternatives
LEVERAGE KEY PARTNERSHIPS

Build partnerships outside your organization

In healthcare, key resources are:

1. Peer organizations – non-profit and for-profit
2. State - Dept. of Community Health
3. State - Health Information Exchanges
4. State - Health & Hospital Association
5. HiTrust & NH-ISAC
6. Federal – Health & Human Services
7. Federal – FBI & InfraGard
Resources are ALWAYS constrained

- Reason for risk-based prioritization
- Outsource if necessary, but commodity functions

Encourage/reward innovation (think like there is no box!)

- May increase productivity
- Can help improve morale

Look for external funding

- Federal & State grants may be available
- May be able to participate in outside initiatives
PRACTICAL STEPS FOR A CISO

1. Decide on a framework (ISO, NIST, HiTrust, etc.)
2. Understand business priorities
3. Understand the technical environment and data flows
4. Identify & assess areas of risk
5. Prioritize based on risk and over-communicate
6. Talk with vendors and integrators
7. Educate, educate, educate (users, staff, yourself)
6-STEP SECURITY CYCLE

1. Inventory Business Critical Data
2. Perform a Risk Assessment
3. Develop a Security Strategy
4. Have an Incident Response Plan Ready
5. Implement Policies, Processes, and Technologies
6. Train Workforce

(Source: Healthcare IT News)
TAKEAWAYS
WHO IS THE CISO?

1. Security Leader? IT Leader?  
   YES, Depends

2. Business-Savvy Executive?  
   YES

3. Risk Leader?  
   YES

4. Compliance Leader?  
   Depends

5. Team Leader, Coach, Mentor?  
   YES

6. Therapist?  
   YES

7. McGyver?  
   YES
Recommendations

1. Understand expectations of you
2. Understand business critical functions/data
3. Understand threat landscape
4. Follow a framework and prioritize by risk
5. Institute governance involving stakeholders
6. Build and leverage your team and NETWORK
7. Adapt as necessary
Strive not to be a success but rather to be of value. -Albert Einstein
Thank You!

Doug Copley
dcopley@forcepoint.com

http://blogs.forcepoint.com
Twitter: @hcare_security
www.linkedin.com/in/dcopley