BREAKING BARRIERS TO
COLLABORATE WITH THE C-SUITE

31st Annual SoCal ISSA Security Symposium

Wendy T. Wu
Vice President

Agenda

+ CISO: Then and Now
+ Who are the Stakeholders and What Do They Care About? (Stakeholder Analysis)
+ How to Engage the Stakeholders?
+ How to Get Support from the Company Executives?
+ Working with Law Enforcement
CISO: Then and Now

The Role of the CISO

Then:
+ Purely IT/technical job
  - System/network admin or CS
+ Reported to CIO only
+ No interaction with other business functions

Now:
+ Role has evolved
+ More complex (or well-rounded)
+ Must be tech savvy + business savvy
+ Must also advise CIO, GC, CCO, Board
Role of the CISO Now

+ Need to understand company assets in order to measure risk/exposure
+ Must have buy-in from the BOD for a robust, effective cybersecurity program
+ Not just budget issues; need leadership to endorse and socialize cyber policy throughout company

Who are the Stakeholders (and What Do They Care About)?
Stakeholder Analysis

What do they care about:
+ Best interest of the company.
+ Business enablement
  - i.e., willing to support if the investment assists them achieve operational/market goals (and security at the same time)

How are they different?
+ Priorities (focus + responsibility)
+ Perspectives
+ Technical expertise and understanding (or the lack thereof)
  - They don’t know what they don’t know

Stakeholder Analysis At a Glance

<table>
<thead>
<tr>
<th>GC</th>
<th>CPO/CCO</th>
<th>CFO</th>
<th>CEO/BOD</th>
</tr>
</thead>
</table>
| + Liability                     | + Concerned with processes that handle sensitive data  
  | + Notice and reporting obligations  
  |  - Regulators  
  |  - Consumers  
  | + Litigation risk  
  | + Outside counsel  
  | + Law enforcement | + Business performance 
  |  + Earnings  
  |  + Forecasting  
  |  + Budgeting  
  | + Answer to shareholders/investors  
  | + Global operations (CEO)  
  | + Growth of company  
  | + Reputation  

STROZ FRIEDBERG
How to Engage the Stakeholders?

How to Engage?

Demonstrate and communicate the value of information security and risk management in financial terms to business executives.
How to Engage?

+ Speak like a business professional, not IT
  - Can’t talk about indicators of compromise or malware
+ Use business terms that are familiar to executives
  - E.g., financial risk, exposure, reputation, productivity
  - Example: companies are moving into or considering transitioning data to the Cloud for financial savings and operational efficiency, but information security is key, as well as benefit.

How to Engage?

+ Changes in global data protection laws and greater regulatory scrutiny can be used to your advantage
  - Companies now must consider devoting greater resources to information security
+ Goal: Make the execs comfortable, if not willing, to spend money on data security
How (not) to Engage?

+ *Warning:* Don’t be a hero, i.e., trying to save the company from all the bad hackers

Phases of CISO Engagement
Build Phase Support

Goal:
Build credibility
(so people will trust your decision-making)

What’s the Approach?

+ Ask for meetings, informal discussions
+ Look for internal training with other business/departments heads
  - Don’t forget Marketing, HR
  - Find out what their objectives are, what matters to them
  - Time consuming but valuable
+ Key: Be proactive. Start discussions before having to make decisions and deal with problems.
What’s the Approach?

+ Find out what has been done, previous assessments and results
  - If nothing, find out why
  - *Don’t be alarmist*
+ Engage with the IT team = people doing the work, first responder
  - When (not if) an incident happens; must work with both sides
+ Need to know critical data
  - Where the data is flowing, who has access/needs to have access

What’s the Approach?

+ Need to understand risk
  - Obtain *independent*, risk-based security assessment
  - Focus on governance and operation
  - Recommend priorities
  - Need *independence* to ensure objectivity
+ Key: must understand that cyber risks extend beyond IT to all areas of the enterprise – compliance, legal, regulatory
+ Need to understand the organization’s tolerance
  - E.g., budget, culture, hierarchy/structure
  - Security measures should not negatively impact productivity
+ Present (and have execs participate) in dialogue around the risk/impact of those findings
Operate Phase Support

Goal:
Obtain support from execs during security operations (and continue to build credibility)

What’s the Approach?
+ Expand your understanding of risk beyond IT
  - Legal, audit, compliance requirements
  - Operations policies
+ Alignment and conflict with audit and compliance
  - Understand that an audit would be based on a specific regulation or standard and determining whether the company is in compliance
  - Need to prioritize security execution above audit where such policies and controls are stronger as a result
Goal:
Obtain support from execs while reacting to cyber incident

What's the Approach?

+ Execs should not be hearing from you for the first time
+ Best chance for success = CISO who can effectively engage with leadership
+ Resources and support will enable security experts to do their job
+ Understand the role of law enforcement
  - When to bring in LE?
  - Pros and cons
Get to Know Law Enforcement

- Opportunities to get to know local LE/FBI cyber before a cyber incident
  - Business Email Compromise Working Group
  - USAO Cyber Summit for GCs, CIOs, CISO
  - Orange County Regional Computer Forensics Laboratory (OCRCFL)
- LE places a high priority on victim interests, avoid re-victimizing through unwarranted disclosure of information
- Some mechanism to protect sensitive information, e.g., grand jury process, protective orders

Working with Law Enforcement

- Need to get information ASAP and in real time
- Data can be destroyed in an instant; important to notify early and give agents access to data
- Agents may have seen the same conduct or indicators of malicious activity in other cases and can make connections to identify possible targets
- Cooperation is critical because the threat you face includes hackers with unlimited resources and/or full backing of their government.
Stroz Friedberg is a specialized risk management firm built to help clients solve complex challenges prevalent in today’s digital, connected and regulated world.

Our focus is on cybersecurity, with leading experts in digital forensics, incident response and security science; investigations; eDiscovery; and due diligence.
Thank You.

Wendy T. Wu
Vice President
T: +1 310.623.3283
M: +1 310.926.5190