Cyber Security in the Commercial Sector
IDC Private Study: Final Report

Steve Conway
Earl Joseph
Bob Sorensen
July 24, 2015
Project Objectives

1. Conduct a number of case studies of US commercial organizations in order to learn:
   - What security problems they have experienced?
   - Changes that they have made to address them
   - New underlying security procedures that they are exploring
   - What they have learned
   - How they deal with outsider and insider threats
   - Who is best in their industry?

2. How do they make the trade-offs between costs $\rightarrow$ better security $\rightarrow$ client impacts/business operations?

3. What new are they concerned about?
Research Approach

1. Create an open-ended set of questions
2. Survey key experts – individual responsible for their security environments or for advising commercial customers on IT security – to obtain main patterns and to identify who is best in major industry sectors
3. Next, survey additional key experts (as in 2.) plus companies representing the best at security in major commercial sectors
4. Map the newly collected information to IDC existing information and analysis – to create the IDC view of the current situation
5. Create the final report slide deck
Final Report (July 24)

- 14 in-depth interviews
  - 6 global IT vendors
  - 2 financial services firms
  - 2 global manufacturers
  - 2 global cloud services
  - 1 online reference service
  - 1 large IT integrator
Main Areas of Concerns Around Security

- Trade-offs between security and easy access
- Access from network edges (suppliers, remote employees, others)
- Heterogeneity (BYOD, multiple OS, public/hybrid clouds, etc.)
Impact of Recent Major Breaches (e.g., Target, Sony) on Your Company

- Elevated concerns but have not led to much action yet in the commercial world
Who In Your Industry Is Best At Dealing with Security?

- Best: FBI, financial services firms (Deloitte, Mandian), large retailers, life sciences firms, large technology firms, large public cloud services. Walmart is outstanding: 150 incident response people at HQ and a forensics lab judged as good as the FBI's.
- Worst: Universities, manufacturers, public utilities
What Do The Best Do That Makes Them Best?

- Hire top talent at top salaries to create and run the security system
- Use proven methods, such as redundant controls and not giving anyone full control. Use ISO, other industry standards
- Create a detailed crisis plan that includes communications/PR.
How Do You Deal with Insider Threats?

- Most respondents worry more about hacking than insider threats, although they see both as important.
- The best screen candidates well at hire, use MLS/RBAC (multilevel security, role-based access control) employee education, entitlement management
How Do You Trade Off between Better Security, Costs, and Business Disruption?

- Many companies want better security but not the increasing operating expenses and immediate productivity loss needed to achieve it.
- The best invest heavily in security to prevent loss of credibility that could kill their businesses.
Is It Worth Encrypting Everything?

- Respondents all agreed this is unfeasible for financial and other practical reasons.
- A few firms encrypt everything in transit, but not everything at rest.
The Most Important Security Threat For Your Organization Today

- The most frequently mentioned threats were “bring your own device” (BYOD) and everything outside the firewall.
Best Practices To Address Security Threats Today

- Use proven methods, such as redundant controls and not giving anyone full control. Use ISO, industry standards.
- NIST standards are seen as comprehensive but hard for most companies to implement; MLS, role-based access control (RBAC) is getting more serious in the private sector.
How You Measure the Effectiveness of Your Cyber Security Program

- Adequate security is in the mind of the beholder.
- Most firms track easy numbers: number of days without incidents, number of blocked/mitigated threats.
- The best firms say these numbers alone are meaningless. Instead, they create their own metrics, such as % of customers protected in a phishing attack.
Importance of Security in Your Supply Chain

- One of the important concerns, along with everything else outside the firewall
- A bigger concern for government than the private sector
Increased Use of Analytics in Cyber Security

- At the discussion stage – not widely used yet
Actual Breaches and Responses

- Once a breach occurs, the damage can’t be undone and the focus is on learning from it (and catching the bad guys)
- The biggest challenge is keeping up with the increasing sophistication of the bad guys
Questions?

ejoseph@idc.com
sconway@idc.com
bsorensen@idc.com