Security Obstacles and Motivations for Small Businesses from a CISO's Perspective

Flynn Wolf - University of Maryland at Baltimore County (UMBC)
Adam J. Aviv - George Washington University
Ravi Kuber - UMBC

flynn.wolf@umbc.edu

Motivations to understand small business CISOs

- Small businesses (SBs) are often a vulnerable population online
- Limited resources for security preparation or incident recovery
  - 25% of hacked SBs declare bankruptcy
  - 10% of hacked SBs close entirely
- Economies of scale in cybercrime allow SB targeting
- SB **Chief Information Security Officer**-type roles (CISOs) experienced with explaining an advanced threat model to non-experts

Research questions

- How do experts translate their model of online risk for non-experts?
- According to CISOs, what factors affect small business security and how well are they understood?
- According to CISOs, what security guidance is available to small businesses and how effective is it?
- What practices are important to instilling better security in small businesses?

Study 1

- Exploratory semi-structured interviews
- (n=8) SB-experienced CISOs view of SB challenges
- Private and federal/state/county level SB consultants and development officers

Study 1 – Findings

- CISOs confirmed SB vulnerability to online threats
- SBs don't understand and invest in IT security
- CISO divided on responsibility for SB IT security shortfalls
- Felt government authored guidance was hard to use but appropriately thorough
- Saw commercial guidance as more efficient but narrow in focus and often solution/profit-driven
- Offered perspectives on best practices for developing security awareness

Study 1 - SBs deemed highly vulnerable by CISOs

- SBs deemed mostly reactive to IT security incidents
- Might learn from operating in "Starbucks and airplanes" (p1.01, CISO consultant to a county-level SB council), but generally unaware and unprepared
- Incidental improvement from IT upgrades
- Some motivated by domain regulation (e.g., finance, medical, accounting)
- Limitations in available sources of security guidance
- Some limited incentives for SBs to improve security for contractual obligations

p1.01 (expert):
"Might be worth it to comply for ten contracts, but not for one,"
"[SBs] do the customer-required [fixes] and may just omit the ones they can't cost-justify."

Study 2

- Structured interviews
- Validate and extend Study 1 themes
- (n=19) SB CISOs
- Notably low recruitment response rates
- Avg. 49 yrs old, 2 female ID, 15 yrs. netsec experience
- Average SB size of 44 employees

Study 2 Structure

- Part 1 themes chosen for validation
  - SB motivations for security improvement
  - Availability of adequate or affordable security education resources
  - SB understanding of IT risk factors
  - Differences in the efficacy of commercial versus government-authored guidance
  - Influences on SB willingness to invest in security improvements.
- Structured 5-point Likert agreement questions, with open-ended discussion

Study 2 - SB motivations and obstacles

- Confirmed view of SBs as too resource-limited and uninformed
- Shared blame assigned for SB vulnerability
  - SBs often not doing enough, relying on hopeful “security through obscurity”
  - Business software and hardware deemed unacceptably flawed

p2.14: [For SBs] …
“the goal is to work on the widget”

p2.01 (IT security supervisor):
[Software companies] “are more interested in getting to deadline and producing the product to get the money to fix the flaws... Let the world find them. And at the same time that puts all of their customers at risk.”

Study 2 - SB motivations and obstacles

- Other motivations and enabling factors
  - IT upgrades and cloud-based SaaS helps
  - Tax incentives unfamiliar
  - News reports and business reputation

Study 2 – Security guidance

- Adequate guidance available, but hidden costs to effective implementation
- Mixed view of government guidance
  - Lengthy and abstract, hard to use
  - Comprehensive and impartial
- Commercial guidance deemed for practical, but profit-motivated

p2.03 (university cybersecurity manager): "[Commercial guidance] too sales-y."

p2.05 (IT Manager, 10 years of experience):
"You have to really extrapolate a lot of what they are trying to say [in government security standards]." "Most people really only find out what those mean when they get audited, right?."

[Government authored security guidance]:
"Brutality to read." (p2.05)
"Buried in standards" (p2.04)
"Ambiguous natural language" (p2.09)
"Gobbeldy goop" (p2.05)

Study 2 – Security guidance formats

- Checklists favored as a concise basis for security reviews, but also deemed too inflexible and abstract

p2.03: “I’m working with auditors everyday...They’ll come in with a checklist and go check-check-check...and I have no idea what they’re actually working with…It’s not actually doing anything…It’s very rigid, very overblown.”

p2.05 (IT security manager): [Checklists] “easy to follow but. . . don’t encapsulate reality.”

- Team-based exercises require extra preparation to provide real training value

p2.03: “Yeah. [Exercises] are just garbage in a lot of instances…They’re pretty ineffective.”

p2.05: [Exercises] “turn vague ideas into reality.”

Implications – Provide more effective security checklists

- Supply rich context
  - Clarify meaning with examples
  - Offer references for follow-up
- Describe intent behind actions
- Provide prioritization scheme

Implications - Timing for optimal security messaging to SBs

- Within short term business processes
  - Preparation for hiring
  - Evaluation for IT upgrades
- Long-term business processes
  - Follow-up to annual tax projections (2-3Q)
  - Investment cycles (2-3rd round)
  - Post product delivery
- Fold into emergency planning

p2.10:
SB security decision require time “to breathe.” Otherwise, too focused on “staying lean and shipping product.”

Implications – Effective labeling of SB security guidance

- Label guidance by target audience to expedite search
  - Level of IT experience
  - IT resources
  - Business domain
- Support prioritization of action items

Implications – Best practices for SB team-based exercises

- Integrate IT and management
- Ground scenarios in a SB's financial specifics
- Ground scenarios closely in a SB's business domain

Thanks & questions

flynn.wolf@umbc.edu