**Shadow IT and the risks to Technology companies**

**Preliminary outline**

1. A note from Mike Thoma
2. Introduction
3. Shadow IT – what it is and why Technology companies should care
   1. Growing popularity of cloud computing
   2. Overwhelming popularity of mobile devices
   3. Overworked/understaffed IT departments
   4. Demands on IT to do more with less
   5. Slow, bureaucratic approval processes for new IT infrastructure
4. Five types of shadow IT that Technology companies should worry about
   1. Lines-of-business (LOB) managers with their own IT budget (can use on any IT resource, bypassing their company’s own IT department)
   2. Outsourcing to cloud vendors (who cannot always be vetted for security and compliance)
   3. Employees using inexpensive personal cloud data stores (Box, Dropbox, iCloud) for reasons of convenience and productivity (which could put sensitive data at risk)
   4. BYOD (smart devices are marketed as consumer products, so they come stock with minimal security configurations)
   5. USB memory sticks (ubiquitous and barely visible. Most employees use them to skirt IT’s security requirements which they find to be overbearing and counterproductive).
5. Shadow IT risk categories that technology companies should be aware of
   1. **Category 1: Technology E&O**
      1. Description
      2. Illustrative Risk Scenarios
         1. A radio company’s contractors install a capacitor incorrectly based on an error in the engineering schematics, causing failures to occur. Between 12,000 and 14,000 units are installed by the time the problem is discovered. Client sues to recover damages resulting from the failures.
         2. A contract system integrator working on a workforce management system misses milestone important deliverables, causing significant delays in production. Contractor accuses the client of scope creep--slow material changes to size, scope, and requirements of the project. The client fires the contractor, then sues for lost profits due to contractor non-delivery.
      3. Actions to Mitigate
   2. **Category 2: Cyber and intellectual property**
      1. Description
      2. Illustrative Risk Scenarios
         1. LOB leader uses his own budget to hire consultants to write a web app. Contractor unknowingly programs security holes into the app due to poor coding practices. Hackers exploit the vulnerabilities, steal credit card names and numbers. Company is sued for not adequately protecting sensitive data.
         2. Employee uses a 4GB memory stick at work to transport large files that would otherwise be quarantined by company email. She takes inserts the stick into her home PC which is infected with a Trojan, then brings the same stick to work the next day. Trojan infects the entire network, sends sensitive information back to hacker group who uses that data to make fraudulent purchases from online retailers.
         3. Department in a remote location built his own wifi subnet at work using a Fritz!Box. He didn’t disable the router’s DHCP server, so it started assigning conflicting IP addresses to other departments, bringing the entire company down. Company lost a lot of revenue as a result of the outage (this actually happened).
      3. Actions to Mitigate
   3. **Category 3: Bodily Injury**
      1. Description
      2. Illustrative Risk Scenarios
         1. Employee of a manufacturing company brings his tablet to work which is infected, unbeknownst to him. The virus permeates the shop floor subnet and causes robotics to perform erratically, injuring assembly line workers.
         2. Municipal employee uses real-time technical support via browser-based chat window on his personal PC he brings to work. His PC isn’t a member of the network, so he doesn’t have the same security software. A hacker intercepts his chat window, impersonates tech support and encourages him to divulge sensitive credentials (social engineering) he then uses to hack into the city’s traffic control system, causing accidents and injuries.
         3. A contract software developer at a pharmaceutical firm uses his own PC to write code because it is faster than the machine his employer provides him. He visits a site where he becomes infected with malware, which he then connects to his company’s VPN from home. The malware causes the company’s shop floor system to produce drugs with improper quantities of harmful chemicals. The drugs are released to market, causing patients to get sick (and possibly die) from the tainted drugs.
      3. Actions to Mitigate
   4. **Category 3: Extra expenses (see Expense Reimbursement Coverage section in sell sheet)**
      1. Description
      2. Illustrative Risk Scenarios
         1. A cyber-criminal hacks into a company’s point-of-sale system where he steals 50,000 customer names and credit card numbers. Company must hire a breach response firm to locate and fix the vulnerability, notify affected customers, and provide credit monitoring to prevent unauthorized use of customers’ personally identifiable information (PII).
         2. A thief steals a C-level executive’s laptop containing 100,000 donor records for a non-profit organization. National news broadcasts the theft and the parties responsible. Non-profit organization must hire a PR firm to restore donor confidence and control reputation damage.
         3. An organized hacker community overseas gains unauthorized access to a company’s SaaS accounting system, altering the bank routing information to transfer money into the crime ring’s account. Company loses money and securities, and also experiences business disruption due to lack of operating cash.
      3. Actions to Mitigate
6. The last line of defense: Insurance considerations for Shadow IT

**Interviews**

* Kirstin Simonson, Cyber Lead for Travelers Global Technology (2)
* Chris Hauser / Kurt Oestreicher (joint interview)
* Travelers Risk Control person TBD
* Other TBD

**Process**

1. Initial interviews
   1. Kirstin Simonson (including brainstorming on scenarios)
   2. Chris Hauser / Kurt Oestreicher (joint)
2. Develop detailed outline (with scenarios?)
3. Develop first full draft
4. Interviews
   1. Kirstin Simonson
   2. Travelers Risk Control person TBD
   3. Other TBD
5. Develop second draft