SAULT INSURANCE BROKERS ASSOCIATION

OCTOBER 8, 2014

Cyber Risk Insurance

James Cook, CISSP, CPP

What we will talk about?

- What is cyber security
- What the threats are
- Where your offices fit in
- Cyber risk insurance

What is cyber security

- Security of electronic systems. Sometimes called logical security. The Internet plays a big role.
- Not physical security – fences, gates, etc.

Who?

- Eastern European crime syndicates and others
  - Financial gain
  - Bank account information theft – wire transfers
  - Botnets that can be used for other things (SPAM, Denial of Service, etc)

Who?

- Nation States
  - China, Russia, Iran, Iraq, North Korea, USA
  - Individuals
  - Theft of intellectual property
  - Industrial espionage
  - Industrial control system access
  - Terrorism
  - Cyber warfare

Insurance professionals / offices

- Cyber security criminals are interested in you.
- Watch yourself, even at home.
- You are part of your customers' supply chain.
- Your customers trust you. So they will trust an email from you.
- You move large sums of money.

Insurance professionals / offices

- You likely become aware of mergers and acquisitions in the due diligence process
- Example – Potash Corp
  - Australian company BHP Billiton wanted to purchase Potash Corp
  - Chinese were concerned.
  - Reportedly infiltrated networks of accountants, legal, and public relations agencies.
  - Wanted to know what the Potash Corp position was.

Day to day attacks (apply to you and your customers)

- Most organizations have a reasonably strong perimeter.
- Employees are the weakest link.
- Types of attacks – mostly phishing.
  - Employee opening attachments such as from Canada Post
  - Financial intent – Zeus – a botnet that steals bank account info
  - Employees visiting sites that have been infected
    - You visit a site via Google search -> site has malware -> you get infected -> malware talks to command and control servers to get more instructions -> makes a big mess

More day to day

- Typo sites. Ibc.ca vs ibcc.ca
- Security awareness training.
- Be prudent when opening emails, clicking on links, visiting sites.
- Low hanging fruit.
- Every business is being attacked.

Targeted Attack

- Phishing – general purpose, account stealing, etc
- Spear phishing – targeting a company or department
  - Links, Attachments
- Watering holes
  - Web sites frequented by insurance industry professionals – Insurance Bureau of Canada
- Advanced Persistent Threat
- Denial of service
- Extortion

Vulnerability

- A bug in a program
- Criminals and researches find them

Example – buffer overflow

- Program expects a command “open window”
  - Hacker sends “038AF16C89…B7B5CBB030F9A4B7A”
  - Runs past the end of the expected area
  - Runs what she wants
- Sold to others to be exploited to get access

Cyber risk insurance

- Policy to transfer risk from customer to carrier
- Poor stats. Difficulty calculating actuarial numbers
- What is the risk? Industry specific?
- How do you inspect the current security stature?
- Nothing physical to look at.
- Claims have already started.
- Current focus is on private information.

Cyber risk insurance

- There are some audit standards, but apply more to financial risk (SoX).
- PCI helps where credit cards are involved. But not a lot.
- Carriers will start to ask for more proof. At least administrative controls.
- Carriers will hedge risk by over charging for premiums until claims history is available.
- Also increased competition will drive down premiums.

Examples

- Target
  - Supply chain. HVAC contractor – differing opinions. Likely spear phishing.
  - Various reports, but HVAC system may have been connected to Point of Sale network.
  - Point of Sale system
  - Malware scraped unencrypted credit card numbers while in memory
  - Data exfiltration was timed to coincide with Black Friday so no spike was noticed
  - Continued to run during the busy retailer season.

More examples

- Home Depot
  - Point of Sale infection
  - Still being investigated
- Reputational risk (no one is covering this yet)
- Stock market (Target lost as much as 14% of value at one point)
- Chip and PIN transactions starting in USA. Escalating bank fraud costs.
- Cost of credit protection for customers

Things to think about

- Retail is a big target – anything that handles credit card data
- Other personal identifiable information – Health care (SSN / SIN)
- For intellectual property theft, may not know for months or years. How to quantify damage in order to make claim?
- An official claim may have to show up on SEC or other regulatory filings if damage is material.

More things to think about.

- Involvement of law enforcement. Fear of having IT assets seized as part of investigation.
- Poor relationship government / private in USA. Better in Canada.
- Stigma not as bad as it once was, so likely more claims overall.
- A large attack may force a company to cease operations permanently
  - Eg. source code vault, cloud, all instances deleted.

Lots of things to think about.

- Use a single carrier for property, liability, E&O, and cyber risk.
  - Avoids carriers trying to transfer responsibility for a claim.
  - Avoids adding riders to each class,
- Different carriers are using different terminology. Difficulty making an apples to apples comparison.

QUESTIONS?

http://cookit.ca/index.php/articles

brokers@cookit.ca