Navigating Cyber Security in Engineering

Chris Wilkerson, Greyling / ACEC Business Insurance Trust
Jeff Connelly, Greyling
CYBER CRIME IS BIG BUSINESS AND EXPANDING

- Cyber crime has developed into a Multi-Trillion Dollar industry
- Crime-as-a-service
  - Mature and Profitable Business Model – with same level of professionalism, discipline and structure as a legit business
  - Some “organizations” have as many as 80,000 people w/ “global footprint”
  - Exhibit “corporate behavior:” Supply Chains, Call Centers, Help Desks!
  - Selling Goods (hacking software $100-$500) and Services (Denial of Service-as-a-service, Ransomware-as-a-service...)
- Highly profitable + low risk of being caught
  - Ransomware Return-on-Investment 1500%+
  - Skilled hacker can make $80K in 30 days – off initial investment of $5K
  - Average age of a hacker today is 35 years old – people choose this as a “profession”!

TRENDS IN RANSOMWARE

- Shift from “Smash & Grab” to “Big Game Hunting”
  - More targeted attacks
  - Bigger, customized demands
  - Based on specific financial information
- One-Two-Punch: Ransomware + Data Breach
  - Ransomware becomes just a “part” of the attack
  - Hackers spending more time “inside” the victim’s system before unleashing the ransomware, accessing other information, harvesting credentials, releasing banking trojans
    - Makes “retroactive date” of insurance critical
    - Emphasizes need for active risk monitoring and management
TRENDS IN SOCIAL ENGINEERING

$70,960
Average Cost of a Business Email Compromise Claim (Beazley Data)

• How are criminals getting in?
  – Brute Force
  – Buying credentials
  – Malware
  – Sophisticated fishing and engineering

PANDEMIC IMPACT TO CYBER THREAT LANDSCAPE

• Remote Environment => New Threat Landscape
  – Spike in Social Engineering & Ransomware
    • Sophisticated, Targeted Attacks (Specific Data)
    • Larger Demands
    • Easier Access
  – Implications to IT Governance
    • Controls are critical (MFA, VPN, malware protection, backup and recovery procedures)
WHAT HAPPENS POST-BREACH OR EVENT?

INVESTIGATION
- Retain privacy counsel
- Determine what was impacted (forensics)
- Determine laws that might apply/notification deadlines
- Potentially involve law enforcement

RESPONSE
- Notify impacted individuals/ offer identity theft assistance
- Notify relevant regulators
- PR firm

REGULATORY INVESTIGATIONS & LAWSUITS
- 3rd Party Privacy lawsuits
- Regulatory investigations

REPUTATIONAL FALL-OUT
- Brand damage/lost trust/bad PR
- Lost customers
- Leadership impact

CYBER REGULATION TRENDS
Emerging Risk: Privacy Regulations

- International and U.S./State-Level Momentum for “comprehensive privacy bills” at an all time high right now
  - General Data Protection Regulation (GDPR) implementation in May 2018 for European Union was a turning point
- Shift from “breach-based” privacy regulations to broad based privacy regulations
- Many U.S. States with breach regulations dating to 2003-2007 have 2018-2020 amendments with heightened requirements:
  - Arizona, Arkansas, Colorado, Connecticut, Delaware, Iowa, Louisiana, Maryland, Massachusetts, Michigan, New Jersey, Oregon, Texas, Utah, Virginia, Washington
  - AND New York, with the Stop Hacks and Improve Electronic Data Security Act (“SHIELD” Act), signed July 25, 2019 and effective 10/23/19 (breach notification) and 3/21/2020 (data security)

N.Y. SHIELD Act: Breach Notification

- Expanded definition of “private information”
  - Now includes biometric information, username/e-mail address in combo with password or security question/answer, account number, credit/debit card number
  - Previously SSN, driver’s license or other ID card number, or account/CC/DC number in combination with security code or password, when combined with other personal information
- Expanded definition of “breach”
  - Now includes “unauthorized access” to data
  - Previously was limited to “acquisition” of data
- Expanded territorial scope
  - Breach notification requirement expanded to any person or business that owns or licenses private information of New York resident
  - Previously limited to those conducting business in NY
POST-COVID CYBER INSURANCE MARKET

• U.S. Cyber Market:
  – 2002: $100M in Gross Written Premium
  – 2017: Approximately, $4.5 BILLION
  – 2025: $20 BILLION

• Pandemic “Market Correction”
  – UNDERWRITING (Public domain scans, vetting of Ransomware controls, conference calls with management / IT)
STANDALONE CYBER INSURANCE OVERVIEW

FIRST PARTY
The Insured’s assets, including:

• Loss or damage to digital assets
• Data recovery/restoration
• Business interruption from network downtime
• Costs of Forensic Investigations
• Notification & Call Center Expense
• Credit monitoring services
• Cyber Extortion & crime
• Consequential Reputational Harm
• Public relations/crisis management

THIRD PARTY
Information of others, including:

• Civil liability actions (class or single plaintiff): defense costs as well as judgments and/or settlements
• Security & Privacy Liability
• Multi-media liability, to cover investigation, defense costs and civil damages arising from defamation, breach of privacy or negligence in publication in electronic or print media
• Fines and penalties incurred as a result of a regulatory action
• Payment Card Industry (PCI) claims
• Notification/Breach Response requirements

SOURCES OF CYBER INSURANCE COVERAGE

• Standalone Cyber Insurance
  – Third-Party Liability Coverage
  – First-Party Notification, Restoration, Response, and Interruption Coverage
• Professional Liability Insurance
  – Third-Party Liability Coverage
  – Scope of coverage and availability varies widely
  – Some still tie coverage to providing professional service
• Commercial Crime
  – Loss of money due to social engineering
  – Typically with sublimits like $100k or $250k
• Property – Electronic Data Protection/Restoration Coverage
What triggers Business Interruption coverage under a Cyber policy?

- Income loss (net profit) resulting directly from a **Cyber Incident**
  - Ransomware
  - Failure of your Network or a contracted 3rd Party IT provider

- Consequential Reputational Fallout

- Subject to Waiting Period

Mind policy sublimits

- “Dependent” Business Interruption

- System Failure

- OFAC
Architecture firm’s data and e-mail servers hijacked and locked down late on Friday
Notice to cyber insurer’s reporting hotline, with mitigation started Friday evening
Breach response consultants on-site Monday morning
Firm decided to pursue recovery of data from redundancy rather than pay ransom
Covered loss under the policy included business interruption / data recovery costs, forensics, and legal services
Claim: ~$900,000, after $10k policy retention
• Engineering firm moves cyber coverage as of January 1, 2019 to London insurer that includes $500k of social engineering coverage, as per Greyling’s recommendation
  – Also has $100k of social engineering coverage in crime policy, but with higher deductible
• In March 2019, Finance department receives a request, allegedly from another employee in a senior financial position, to update bank account information used to hold funds for payroll in UAE. Pursuant to this request, the firm transfers approx. $300k to a fraudulent 3rd party account.
• Between lost funds, breach response, and restoration, claim is $480k, excess of $10k deductible
• Premium on policy: $3,471