The Security Triangle

Security

Functionality

Ease of Use
Everyone is a Target

• 98% of organizations experienced cyber attacks in 2016. (Radware Global Application & Network Security Report)

• 62% of all cyber attacks are against small and mid-sized businesses, about 4000 per day. (IBM Security)

• Over 1 billion credentials stolen last year, 3x greater than the previous high in 2013. (Verizon Data Breach Investigations Report)
Ransomware

• “There are estimates that the total damages due to ransomware will reach approximately $5 billion in 2017.” (Acalvio Senior Director Abhishek Singh to SC Media)

• Over $1 billion in ransoms were paid last year. (FBI Internet Crime Complaint Center)

• Last year, 49% of all companies surveyed suffered at least one cyber ransom incident. (Radware Global Application & Network Security Report)
Statistics and Trends

Business Email Compromise / Spear-Phishing

• $5.3 billion in losses due to BEC from October 2013 to December 2016 (Internet Crime Complaint Center)

• Over 400 companies targeted in BEC spear-phishing campaigns every day. (Symantec Internet Security Threat Report)
Malware and Spyware

• 1 in 131 emails contain malware, the highest rate in 5 years. (Symantec Internet Security Threat Report)

• “25% of organizations surveyed monthly were infected by [spyware].” (Cisco Security Research)

• Citadel Banking Trojan - malware offered for sale to interested criminals. Harvests bank credentials from victims, has caused $500 million in losses and counting.
Google Docs Phishing Scam

• Emails appearing to be legitimate Google Doc sharing requests from other users you know asking you to grant permission for a “Google Drive” app to access your email and contacts.

• Affected over 1 million victims.
Recent Examples

Google Docs Phishing Scam

Named Google Docs

Uses official logo
Recent Examples

Google Docs Phishing Scam

Google Docs would like to:

Developer info

email: eugene.pupov@gmail.com
Clicking "Allow" will redirect you to:
https://googledocs.docscloud.info/g.php
Recent Examples

Other Examples

• WannaCry
• NotPetya
• Mirai Botnet
Big Issues

• Delayed or Neglected Patching

• Insecure Configurations

• Social Engineering

• Emerging: Insecure IoT Devices

• Emerging: PDoS / Phlashing / Bricking
Incident Response Steps

• **Discovery** - a breach is detected or reported by an internal or external source and is escalated within the organization.

• **Analysis** - IT, cybersecurity, and forensic experts determine what happened.

• **Containment** - Ensure the breach is not ongoing, identify and contain the damage.

• **Eradication** - Address the vulnerabilities that led to the breach, eliminate the threat from the environment.

• **Recovery and Post Incident** - Restore normal working operations, perform post-mortem evaluations.
Cyber Incident Costs

• Legal and Regulatory Consequences
• Communications
• Customer Concessions
• Business Interruption
• Other Costs
Cyber Incident Costs

The Numbers

• One instance of a single PHI record compromised cost almost $2 million. (NetDiligence Cyber Claims Study)

• $7.35 million average total cost of breach. 5% increase, a record high.*

• $225 average cost per lost or stolen record. 2% increase, a record high.*

• $690,000 is the average cost to a small business to clean up after a cyber attack. Over $1m for middle market.*

• $4.8 Million Transfer in Medidata Case.

* IBM Security and Ponemon Institute Cost of Data Breach Study
Cyber Incident Costs

Cost Allocation

- Lost Customer Business: 41%
- Legal Defense and Legal Compliance: 20%
- Investigations and Forensics: 16%
- Customer Acquisition Cost: 8%
- Public Relations, Communications: 8%
- Auditing and Consulting: 4%
- Service giveaways, discounts, identity protection: 3%

* IBM Security and Ponemon Institute Cost of Data Breach Study
Cyber Incident Costs

Targeted Industries

Radware Ring of Fire from the Radware Global Application & Network Security Report
Common Problems

- Inadequate InfoSec Policy & Procedure
- Data Hoarding
- IT Not Following Security Best Practices
- Weak Password Practices
- Ignorance is NOT bliss!
Types of data breach costs and the insurance policies’ response

1) First Party Coverages

2) Third Party Coverages

3) Remediation Costs

4) Combined and separated “webs” of insurance policies.
## Network security and privacy GAP analysis

<table>
<thead>
<tr>
<th>1st party privacy/network risks</th>
<th>Property</th>
<th>General liability</th>
<th>Crime</th>
<th>K&amp;R</th>
<th>E&amp;O</th>
<th>Network security &amp; privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical damage to data only</td>
<td></td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Virus/hacker damage to data only</td>
<td></td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Denial of service (DOS) attack</td>
<td></td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Business interruption loss from security event</td>
<td></td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Extortion or threat</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Employee sabotage of data only</td>
<td></td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Impostor fraud</td>
<td></td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3rd party privacy/network risks</th>
<th>Property</th>
<th>General liability</th>
<th>Crime</th>
<th>K&amp;R</th>
<th>E&amp;O</th>
<th>Network security &amp; privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft/disclosure of private information</td>
<td>✗</td>
<td></td>
<td>✗</td>
<td>✗</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Confidential corporate information breach</td>
<td>✗</td>
<td></td>
<td>✗</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Technology E&amp;O</td>
<td>✗</td>
<td></td>
<td>✗</td>
<td>✗</td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Media liability (electronic content)</td>
<td>✗</td>
<td></td>
<td>✗</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Privacy breach expense and notification</td>
<td>✗</td>
<td></td>
<td>✗</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Damage to 3rd party’s data only</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Regulatory privacy defense / fines</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Virus/malicious code transmission</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

- No Coverage ✗ - Possible Coverage ✓ - Coverage
• Setting up protocols
• Interfacing with the insurers and counsel
• Communication, billing, etc.
• Strategies for mitigating transactional costs
• “Setting priorities” among multiple insurers in the coverage “webs”. 
Monoline or Package?

Coverage Pitfalls to look for:

• Employee Claims
• Personal Injury
  - Carve back of bodily injury exclusion
• Independent Contractors
• Data in any format
• Third Party Vendors (On & off site)
• Theft of corporate information
  - Confidentiality agreements required?
Potential Exclusions

- Failure to maintain or upgrade their security
- Failure of software security to match that reported on app
- Unencrypted Device or Wireless Signal Exclusion
- Actions of independent contractors or third party vendors
- Bodily Injury Exclusion
- Withdrawal of software or technical software by a vendor
- Chargeback Exclusion (offset by Credit Card company)
- PCI Exclusion
- Wild Virus Exclusion
- Actions by rogue employees
“Cybercrime costs will grow to $6 trillion annually by 2021.”

–Cybersecurity Ventures
Questions?