Knowing What Happened is Only Half the Battle
Introduction

• Grayson Lenik, MCSE, GCFA
• Director of Incident Response and Digital Forensics for Nuix Cyber Threat Analysis Team (CTAT)
• Data Breach Investigator by trade
• Regular presenter and instructor
Agenda

- Data Breach Landscape
- CTAT Response
- Preparing for the worst
- The rest of the battle
- Conclusion
Data Breach Landscape
Data Breach Landscape

WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Huang Zhenyu  Wen Xinyu  Sun Kailiang  Gu Chunhui  Wang Dong
As reported by the 2013 Europol Serious & Organized Threat Assessment, the “Total Global impact of Cybercrime has risen to US $3 Trillion, making it more profitable than the global trade in marijuana, cocaine and heroin combined.” This growing cost of cyber crime partially reflects the different laws that define countries’ breach disclosure policies. For example, whereas the United States has mandatory disclosure laws, the European Union has none.

European-based companies that have been affected by an incident, including TK Maxx, Loyaltybuild, Stay Sure and CEC Bank, are therefore under no obligation to notify their customers of an incident. This lack of visibility may limit the affected company’s incentives to invest in detection measures that facilitate a timely response.
<table>
<thead>
<tr>
<th>Company</th>
<th>Number of Records Breached</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHS Community Health Systems, Inc.</td>
<td>350,000 Records Breached</td>
</tr>
<tr>
<td>Michaels</td>
<td>280,000 Records Breached</td>
</tr>
<tr>
<td>goodwill</td>
<td>4,5 Million Records Breached</td>
</tr>
<tr>
<td>Dairy Queen</td>
<td>2.6 Million Records Breached</td>
</tr>
<tr>
<td>Neiman Marcus</td>
<td>868,000 Records Breached</td>
</tr>
<tr>
<td>Sally Beauty Supply</td>
<td>600,000 Records Breached</td>
</tr>
<tr>
<td></td>
<td>350,000 Records Breached</td>
</tr>
<tr>
<td></td>
<td>280,000 Records Breached</td>
</tr>
</tbody>
</table>
These nine (9) breaches alone represent 215,198,000 records stolen. By way of comparison, that equates roughly to the entire population of:

- Shanghai, China
- Karachi, Pakistan
- Beijing, China
- Delhi, India
- Tianjin, China
- Istanbul, Turkey
- Lagos, Nigeria
- Guangzhou, China
- Mumbai, India
- Moscow, Russia
- Dhaka, Bangladesh
- Cairo, Egypt
- Sao Paulo, Brazil
- Tokyo, Japan
- California
- Texas
- Florida
- New York
- Illinois
- Pennsylvania
- Ohio
- Georgia
- North Carolina
- Michigan
- New Jersey
- Virginia
- Washington
- Massachusetts
- Arizona
In the News - Data Breach Landscape

21 Million Records Breached

40 Million Records Breached
Cost per record is up again.
In the US:
$217 per record up from $201

Canada is close behind at $207

Average cost per data breach is $3.79 million

Canada joined the countries polled in the Ponemon* study!

*http://www-03.ibm.com/security/data-breach/
CTAT Responds

• Nuix CTAT has a slightly different approach
• Not an occupying force
  – Smaller number of responders with high skill levels and years of experience
  – Diverse skill sets on each response team
    • Including scripters, coders, pen-testers
  – Allows us to be more agile, respond faster, keep costs down for customers
CTAT Responds

• Why bring a pen-tester on a breach response?
  – Generally, they have very high technical skill levels
  – Knowledgeable about current tactics and threats
  – “If it were me” mentality that assists in defining investigation scope
  – Can pinpoint major security flaws while on-site and assist with rapid remediation
• No really, it works
  – Last year we worked a data breach case for a major media organization
  – On-site response consisted of a senior incident responder (forensic specialist) and a senior network penetration tester
  – During initial discovery meeting and resource gathering session, pen tester started hammering away to see what creds and resources they could gain access to once “inside”
  – 20 minutes in with giant sticky notes on the walls to detail attack flow, pen-tester giggles
  – Domain Admin escalation due to weak authentication mechanisms
CTAT Responds

• No really, it works, cont’d
  – Investigation pinpoints initial beachhead and that info is turned over to pen-test
  – Pen test finds original vulnerability and several others within minutes
  – Remediation occurs while team is still on-site
  – Reporting completed
  – Customer is happy enough that they schedule annual pen tests and buy retained forensic hours.
Preparing for the Worst
Preparing for the worst

• If you fail to plan, you are planning to fail
  – Have a Breach Response Plan and CSIRP
  – Test those plans
    • Preferably not during a live breach ;)

• Tabletop exercises

• Scenario creation with live analysis and reporting labs
The Rest of the Battle – Post Breach blues
The Rest of the Battle

• You had a plan, you had layers of security, and you tested, tested, tested. But a breach still happened. You’ve recovered from the incident but there’s still a lot of work to be done.
  – Regulatory concerns
  – Legal morass
  – Breach Notification
  – After action and lessons learned
Preparing for the worst

- Regulatory Inquiries
  - SEC / FTC inquiries
    - After a breach, expect the SEC or the FTC to launch an inquiry
    - Section 5(a) of the FTCA – 15 U.S. Code § 45 - “Unfair methods of competition unlawful; prevention by Commission”
    - Recent ruling by the US Court of Appeals, 3rd Circuit ruled that hacked companies can be sued by the FTC
  - HIPAA/HHS OCR inquiries
    - If the breach involves a covered entity or business associate, expect scrutiny from HHS/OCR
    - Scrutiny extends well beyond the breach
    - Fines and penalties can be assessed
Preparing for the worst

• Regulatory Inquiries
  – Attorney General investigations
    • Attorneys general are very active
    • Can also assess fines and penalties
  – Additional contributing cast members
The Rest of the Battle

• 50 States, 50 different notification laws
• We have vetted partnerships with experienced data breach legal teams
The Rest of the Battle

• After Action
  – Learn from your response
  – We can help you decipher what went right and what went wrong
  – Reinforce the good, change the bad with policy and action
Breaches will happen
The legal, social and financial repercussions are daunting
You don’t have to go it alone!
  – Trusted experts
  – Vetted partnerships
  – Experienced teams
Thank You!

FIND OUT MORE:

- twitter.com/nuix
- facebook.com/nuixsoftware
- linkedin.com/company/nuix
- youtube.com/nuixsoftware
- blog.nuix.com
nuix