DETECTING AND RESPONDING TO CYBER ATTACKS IN HEALTHCARE

Gabriel Doncel
Director Information Security
Drexel University
Gabriel Doncel MBA MS CISSP

Director Information Security
Drexel University / Drexel College of Medicine

Gabriel Doncel joined Drexel University in 2019 where he is currently Director of Information Security. He is also part of the University of Delaware and Wilmington University Adjunct Faculty. As a member of the Information Security team at Drexel, and working closely with the campus community and outside parties, his focus is to protect the people, information and systems of Drexel University. Prior to joining Drexel, Gabriel was Cybersecurity Resiliency Program Manager at Christiana Care Health System. He earned a Bachelor of Science degree in Computer & Network Security from Wilmington University, a Master of Science degree in Information Systems and Technology Management, and a Master in Business Administration, both from the University of Delaware.

Certifications include: CISSP, C|CISO, CEH
Drexel University

Founded in 1891 in Philadelphia
• Three Philadelphia campuses and other regional sites.
• The Academy of Natural Sciences of Drexel University, the nation’s oldest major natural science museum and research organization.

Enrollment
• 25,000 total students

Academic Offerings
• Over 200 degree programs
• 15 colleges and schools

Technology Leadership
• First university to require all entering students to have microcomputers (1983)
• First major university to operate a fully wireless campus, indoors and out (2000)

Mission
Drexel University fulfills our founder’s vision of preparing each new generation of students for productive professional and civic lives while also focusing our collective expertise on solving society’s greatest problems. Drexel is an academically comprehensive and globally engaged urban research university, dedicated to advancing knowledge and society and to providing every student with a valuable, rigorous, experiential, technology-infused education, enriched by the nation’s premier co-operative education program.
Agenda

• We Are Under Attack!
• Visibility
• Incident Management
• Workflows and Playbooks
• Threat Intelligence
• Collaboration
• Trends
• Questions?
WARNING!

We're Under Attack!

MAJOR HEALTHCARE BREACHES

- Anthem Blue Cross
  78.8 Million affected
- Premier Blue Cross
  11+ Million affected
- Excellus BlueCross BlueShield
  10+ Million affected
- TRICARE
  4.9 Million affected
- UCLA Health
  4.5 Million affected
- Community Health Systems
  4.5 Million affected
- Advocate Health Care
  4+ Million affected
- Medical Informatics Engineering
  3.9 Million affected
- Banner Health
  3.62 Million affected
Hackers will target any business, but the most vulnerable have also proven to be the most heavily affected.

Verizon Data Breach Investigations Report (DBIR)

<table>
<thead>
<tr>
<th>Who’s behind the breaches?</th>
<th>What tactics are utilized?</th>
</tr>
</thead>
<tbody>
<tr>
<td>73% perpetrated by outsiders</td>
<td>48% breaches featured hacking</td>
</tr>
<tr>
<td>28% involved internal employees</td>
<td></td>
</tr>
<tr>
<td>2% involved partners</td>
<td></td>
</tr>
<tr>
<td>2% featured multiple types of breaches</td>
<td></td>
</tr>
<tr>
<td>50% of breaches were caused by criminal groups</td>
<td></td>
</tr>
<tr>
<td>12% of breaches involved state-affiliated entities</td>
<td></td>
</tr>
<tr>
<td>68% of breaches took months or longer to discover</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who are the victims?</th>
<th>What are other commonalities?</th>
</tr>
</thead>
<tbody>
<tr>
<td>24% of breaches affected healthcare organizations</td>
<td>49% of non-POS malware was installed via malicious email</td>
</tr>
<tr>
<td>15% of breaches involved accommodation and food services</td>
<td>76% of breaches were financially motivated</td>
</tr>
<tr>
<td>14% were breaches of public sector entities</td>
<td>13% of breaches were motivated by the gain of strategic advantage (espionage)</td>
</tr>
<tr>
<td>59% of victims are categorized as small businesses</td>
<td>68% of breaches took months or longer to discover</td>
</tr>
</tbody>
</table>
Visibility

• Increasing number of vendors in the security space!
  – Commercial
  – Open-source
  – In-house

• Data Aggregation

• Bi-Directional integrations where appropriate
  – Future Response Capability
## Incident Management

- Discovery / Reporting
- Response
- Investigation
- Recovery
- Follow-up

<table>
<thead>
<tr>
<th>Maturity level</th>
<th>Ad hoc</th>
<th>Dedicated part-time</th>
<th>Full-time</th>
<th>SOC/IR+</th>
<th>Strategic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>As needed</td>
<td>1-3 specialization</td>
<td>2-5 formal roles</td>
<td>~10 Shifts (possible 24x7)</td>
<td>15+ Intel, SOC, and IR teams</td>
</tr>
<tr>
<td>People</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1-3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>specialization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chaotic and relying on individual heros reactive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>General purpose run book</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tribal knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIEM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sandboxing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CMM equivalent</td>
<td>Initial</td>
<td>Repeateble</td>
<td>Defined</td>
<td>Managed</td>
<td>Optimized</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continuous monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Endpoint forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tactical intelligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Malware analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Additional intelligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IT operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intel-IR drives security program</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Strategic intelligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Coordination with physical security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Workflows and Playbooks

• Based on experience
• NIST.SP.800
  – Brute Force
  – Web / Email
  – Loss or Theft of Equipment
  – Telecommuting Compromise
• Utility / Facility failures
• Natural disasters
• Table-top exercises
Threat Intelligence

- Aggregation of indicators of compromise (IOCs)
- Relevant
- Integration into existing tools
  - Built into the tools
  - 3rd parties
- Visibility along the Cyber Kill Chain®
- Subscription models
  - Free
  - Paid
  - Exchange
Collaboration

• **Internal to your organization**
  – Infrastructure, Privacy, HR, Marketing, Legal
  – Physical Security, Facilities

• **External**
  – Law enforcement (Infragard)
  – Department of Health and Human Services
  – ISAC (H-ISAC / REN-ISAC)
  – Cyber-Insurance provider
  – Regional groups
  – Old style networking!

• **Two-way!**
Trends

- Cybersecurity staffing issues
- Vendor consolidation and alliances
- Social attacks
- Ransomware and botnets
  - IoT as vectors
- Managed services / Cyber vSOC
- Security Orchestration, Automation and Response (SOAR)
- Endpoint Detection and Response (EDR)
- Cloud Workloads
Metrics

Servicenow CISO Dashboard
THANK YOU!

QUESTIONS?