Cybersecurity Essentials for Ops
Cybersecurity: 201

Hartford Foundation
For Public Giving
About Community IT

100% Employee Owned

Advancing mission through the effective use of technology.
Poll – Org Size

How many staff do you have

- 1-10
- 11-29
- 30-50
- 50+
- 50+
Poll – Role with IT

What is your role at the organization?
- End User
- I am the IT person
- I manage our IT function
Cybersecurity Landscape

Cybersecurity Playbook

Putting it into Action
IC3 Complaint Statistics

Last Five Years

2,211,396 TOTAL COMPLAINTS

<table>
<thead>
<tr>
<th>Year</th>
<th>Complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>298,728</td>
</tr>
<tr>
<td>2017</td>
<td>301,580</td>
</tr>
<tr>
<td>2018</td>
<td>351,937</td>
</tr>
<tr>
<td>2019</td>
<td>467,361</td>
</tr>
<tr>
<td>2020</td>
<td>791,790</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>Losses</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>$1.5 Billion*</td>
</tr>
<tr>
<td>2017</td>
<td>$1.4 Billion*</td>
</tr>
<tr>
<td>2018</td>
<td>$2.7 Billion*</td>
</tr>
<tr>
<td>2019</td>
<td>$3.5 Billion*</td>
</tr>
<tr>
<td>2020</td>
<td>$4.2 Billion*</td>
</tr>
</tbody>
</table>

$13.3 Billion TOTAL LOSSES*

(Rounded to the nearest million)
State of Nonprofit Cybersecurity

- 60 percent of organizations either did not know or don’t have a policy in place that would identify how they would handle risk, equipment usage and data privacy.
- 74 percent of organizations have not implemented Multi-Factor Authentication.
- 46 percent reported that they used unsecured wireless and Bluetooth devices.
- 92 percent reported that staff could access org email, files and information systems from personal devices.
Nonprofit Cybersecurity Incidents

![Graph showing trends in nonprofit cybersecurity incidents from 2018 to 2020. The graph includes categories such as Spam, Malware, Spear Phishing, Virus, Ransomware, Account Compromise, Advanced Persistent Threat, and Wire fraud. The number of incidents varies for each category over the years.]
Cybersecurity - Adversaries
HOW MUCH IS BUSINESS DATA WORTH TO BAD ACTORS?

6 BILLION DIGITAL RECORDS EXPOSED IN 2018

43% OF ALL BREACHES INVOLVED SMB VICTIMS

CREDIT CARD INFO
$2-$5 (per record)

CUSTOMER PII
$20-$450 (per record)

EMPLOYEE PII
$20-$450 (per record)

MEDICAL RECORDS
$20-$50 (per record)

SALES/FINANCIAL INFO
Competitive Value

PROPRIETARY INFO
Competitive Value

Per the Verizon Data Breach Investigation Report
Estimated data values from Sociable
OUR APPROACH TO CYBERSECURITY

NextGen Tools

Identity  Data  Devices  Perimeter  Web

Security Awareness

Security Policy
Cybersecurity Controls

- Proactive
- Optimized
- Foundational
QUESTION

• Does your organization have a formal budget for IT and Cybersecurity
  • Ad Hoc Budgeting
  • We budget for IT only
  • We budget for IT and cybersecurity
  • Holistic and strategic multi-year budgeting
BUDGET

• To help provide some context to these recommendations we’ve assigned a scale from $-$$$$.
• These costs for what a 25-person organization would incur over the course of a year.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>$0-$2,000</td>
</tr>
<tr>
<td>$$</td>
<td>$2,000-$8,000</td>
</tr>
<tr>
<td>$$$</td>
<td>$8,000-$15,000</td>
</tr>
<tr>
<td>$$$$</td>
<td>$15,000+</td>
</tr>
</tbody>
</table>
Foundational

Policy
- IT Acceptable Use
- Data Privacy
- Incident Response
- Insurance Review

Security Awareness
- Free or ad hoc Staff training
IT Acceptable Use

- Includes overview of technology use at the Organization
- Incorporates a list of information systems
- Establishes basics of password and access
- Defines some data retention guidelines
**Free IT Training Resources**

• Stop Think Connect
  • [www.stopthinkconnect.org](http://www.stopthinkconnect.org)

• Community IT
  • [www.communityit.com/resources](http://www.communityit.com/resources)
  • [www.youtube.com/CommunityIT](http://www.youtube.com/CommunityIT)
Foundational

Technology Controls

- Multi Factor Authentication
- Password Manager
- Backups
- OS and Third-Party Updates
- Antivirus
- Spam Filtering
- Business Email Compromise Protection
- Website protection
Poll – Foundational IT Controls

• We've implemented the following controls at our org:
  • Multi Factor Authentication
  • Password Manager
  • Backups
  • OS and Third-Party Updates
  • Antivirus
  • Spam Filtering
  • Business Email Compromise Protection
  • Website protection
Account takeover prevention rates, by challenge type

**Device-based challenges**
- On-device prompt: 100% for Automated bot, 99% for Bulk phishing attack, 90% for Targeted attack.
- SMS code: 100% for Automated bot, 96% for Bulk phishing attack, 76% for Targeted attack.
- Security key: 100% for Automated bot, 100% for Bulk phishing attack, 100% for Targeted attack.

**Knowledge-based challenges**
- Secondary email address: 73% for Automated bot, 68% for Bulk phishing attack, 79% for Targeted attack.
- Phone number: 100% for Automated bot, 26% for Bulk phishing attack, 50% for Targeted attack.
- Last sign-in location: 100% for Automated bot, 100% for Bulk phishing attack, 95% confidence interval for Targeted attack.
**Business Email Compromise**

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Upon transfer, the funds are steered to a bank account controlled by the organized.
**Proactive**

**Policy**
- Risk Assessment
- Cyber liability insurance
- BYOD Policy

**Security Awareness**
- Formal LMS system
Cybersecurity Awareness

SMB Nonprofits (1-249 employees)

• Phase 1 (Initial baseline results) – **39.4%**

• Phase 2 (90 days after initial training) – **14.9%**

• Phase 3 (1 year into training program) – **4.8%**
NIST 800-53

- NIST is one cybersecurity framework
- Developed for Federal Agencies & Contractors
- 1683 line spreadsheet of controls
## Prioritized Recommendations

### Top Risk Areas

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR.AT-1</td>
<td>All users are informed and trained</td>
</tr>
<tr>
<td>ID.RA-3</td>
<td>Threats, both internal and external, are identified</td>
</tr>
<tr>
<td>ID.RA-1</td>
<td>Asset vulnerabilities are identified and documented</td>
</tr>
<tr>
<td>DE.CM-3</td>
<td>Personnel activity is monitored to detect potential</td>
</tr>
<tr>
<td>ID.RA-2</td>
<td>Threat and vulnerability information is received from</td>
</tr>
</tbody>
</table>
POLL – Cybersecurity Insurance

• Does your organization have Cyberliablity Insurance?
  • No, doesn't apply to us
  • Not yet, working on our application now
  • Yes, for a year
  • Yes, have had it in place for several years
Cyberliability Insurance

• Distinct from existing insurance policies
• Many controls are now required
  • MFA for everything
  • Managed security
  • Encrypted data
  • Vulnerability scanning
Proactive

Technology Controls

- Single Sign on
- Data Management (DLP)
- BIOS / Driver Updates
- BYOD Control
- Device Encryption
- Endpoint Detection and Response
- Web filtering
Poll – Proactive Controls

• We've implemented the following controls (multiple choice)
  • Single Sign On
  • DLP
  • BIOS & Driver updates
  • BYOD Management
  • Device Encryption
  • Endpoint Detection and Response
  • Web filtering
  • None
Optimized

Policy
- Business Continuity

Security Awareness
- Cybersecurity Assessment
Optimized

Technology Controls

- Device Trust / Zero Trust
- CASB / SASE
- Vulnerability Scanning
- Penetration Testing
- SOC / SIEM
Getting Started

There’s no one right way

- Bottom up: IT takes ownership and leads the process
- Top down: Executive leadership or the Board mandates changes
**Action Steps**

- Review your existing controls
- Develop risk profile
- Incorporate cybersecurity into budget planning
Questions?