Cybersecurity

NCUA Board of Directors – October 2019
Cybersecurity Landscape Overview - Financial Service Target Profile

**Vertical markets under threat**

<table>
<thead>
<tr>
<th>Market</th>
<th>Number of threat actors targeting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services</td>
<td>8</td>
</tr>
<tr>
<td>Gov't/Military</td>
<td>8</td>
</tr>
<tr>
<td>Tech/Entertainment</td>
<td>7</td>
</tr>
<tr>
<td>Telecom</td>
<td>7</td>
</tr>
<tr>
<td>Energy</td>
<td>6</td>
</tr>
<tr>
<td>NGOs/Civil society</td>
<td>5</td>
</tr>
<tr>
<td>Legal</td>
<td>3</td>
</tr>
<tr>
<td>Retail</td>
<td>2</td>
</tr>
<tr>
<td>Healthcare</td>
<td>2</td>
</tr>
</tbody>
</table>

**Note:** Large amount of Personal and Financial Information and actual Monetary targets

*Source Flashpoint*
Cybersecurity Landscape Overview – Attack Methods

Note: Additional layered complexity and persistence still equates to the same predominate root cause

Accenture 2019 Cost of Cybercrime Study
Cybersecurity Landscape Overview – IT Spending

IT Security Spending to Reach a Record $114 Billion in 2018

<table>
<thead>
<tr>
<th>Segment</th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Services</td>
<td>$102b</td>
<td>$114b</td>
<td>$124b</td>
</tr>
<tr>
<td>Infrastructure Protection</td>
<td>$14.1b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Security Equipment</td>
<td>$12.4b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Access Management</td>
<td>$9.8b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumer Security Software</td>
<td>$6.4b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated Risk Management</td>
<td>$4.5b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security</td>
<td>$3.1b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Security</td>
<td>$2.7b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Information Security Software</td>
<td>$2.1b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Security</td>
<td>$0.3b</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Benefits also share increased concentration risk, e.g., business services, cloud providers, managed security services.

Source: Gartner
Cybersecurity Landscape Overview – Talent Management

2016 Cybersecurity Skills Gap

Too Many Threats

- $1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) RECORDS STOLEN IN 2014
- 97% BELIEVE APFS REPRESENT CREDIBLE THREAT TO NATIONAL SECURITY AND ECONOMIC STABILITY
- MORE THAN 1 IN 4 ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK
- $150 MILLION: AVERAGE COST OF A DATA BREACH BY 2020

Too Few Professionals

- 2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY PROFESSIONALS BY 2019
- 3X RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14
- 84% ORGANIZATIONS BELIEVE HALF OR POWER OF APPLICANTS FOR OPEN SECURITY JOBS ARE QUALIFIED
- 1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION’S INTERNET OF THINGS (IoT) DEVICES
- 74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM
- 53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS 6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES
- 77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS A CAREER.
- 89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO HAVE CYBERSECURITY-CERTIFIED EMPLOYEES

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

Sources:
2. ISACA 2015 APT Study, October 2015.
3. ISACA 2015 APT Study.
6. ISACA 2015 IT Risk/Reward Barometer-Member Study.
7. UK House of Lords Digital Skills Committee.

** “Employees” refers to data security professionals at organizations that potentially access to survey respondent’s personal information.


- Highly technical skills e.g. threat hunt team members (Red Team/Blue Team, etc.) vs. leadership/management resources
- Demand more of system administrators, engineers, and programmers by way of Service Management/Delivery
Cybersecurity Landscape Overview – Critical Security Controls (Root Cause)
Cybersecurity Landscape Overview – Resilience

<table>
<thead>
<tr>
<th>Maturity Descriptor</th>
<th>Employment of Security Controls</th>
<th>Security Tailored to Mission</th>
<th>Participate in Information Sharing (threat/vul.)</th>
<th>Response to Cyber Threats</th>
<th>Resilience to Cyber Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 5: Resilient</td>
<td>Augment CSC Based on Mission</td>
<td>Mission Assurance Focused</td>
<td>Real Time Response to Inputs</td>
<td>Anticipate Threats</td>
<td>Operate Through Sophisticated Attack</td>
</tr>
<tr>
<td>Level 4: Dynamic</td>
<td>Augment CSC Based on Mission</td>
<td>Mission Focused</td>
<td>Real Time Response to Inputs</td>
<td>Rapid Reaction To Threats</td>
<td>Able to respond to Sophisticated Attack</td>
</tr>
<tr>
<td>Level 3: Managed</td>
<td>CSC Integrated and Continuously Monitored</td>
<td>Partially Mission Focused</td>
<td>Respond to Information Inputs</td>
<td>Respond to Attacks After the Fact</td>
<td>Protection against Unsophisticated Attack</td>
</tr>
<tr>
<td>Level 2: Performed</td>
<td>Foundational/Critical Security Controls (CSC) Implemented</td>
<td>Mission Agnostic</td>
<td>Inconsistent Response to Information Inputs</td>
<td>Respond to Attacks After the Fact</td>
<td>Some Protection Against Unsophisticated Attacks</td>
</tr>
<tr>
<td>Level 1: No Resilience</td>
<td>Inconsistent Deployment of Security Controls</td>
<td>None</td>
<td>None</td>
<td>No Response</td>
<td>Susceptible to Unsophisticated Attacks</td>
</tr>
</tbody>
</table>

The “when” paradigm

The “if” paradigm
Cybersecurity Landscape Overview – Threat Hunting

**Note:** Informed by the Risk Assessment/Business Impact Analysis

“Know the Business”
Chairman’s Cybersecurity Priorities

- Advancing consistency, transparency and accountability within the cybersecurity examination program;

- Stimulating due diligence for Supply Chain and Third-Party Service Provider management within the credit union sub-sector;

- Assisting institutions with resources to improve operational hygiene and resilience; and

- Ensure NCUA’s systems and collected, controlled, unclassified information are secure.
### Projected Phased Implementation Plan

<table>
<thead>
<tr>
<th>Year</th>
<th>ACET Maturity Assessments</th>
<th>Risk-focused IT Examinations w/ Critical Security Control Emphasis</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>$1B</td>
<td>Pilot</td>
</tr>
<tr>
<td>2019</td>
<td>$1B</td>
<td>Implement</td>
</tr>
<tr>
<td>2020</td>
<td>$100M – $250M</td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td>&lt; $100 Decision Point</td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td>Repeat Cycle</td>
<td></td>
</tr>
<tr>
<td>2023</td>
<td>Baseline/Benchmark</td>
<td></td>
</tr>
<tr>
<td>2024</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2025</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Decision Points**
- **2022**: Repeat Cycle
- **2023**: Baseline/Benchmark

**Key Milestones**
- **2018**: $1B
- **2019**: $250M – $1B
- **2020**: $100M – $250M
- **2021**: < $100 Decision Point

---

**Maturity Assessments**

- **ACET Maturity Assessments**
  - **2018**: $1B
  - **2019**: $250M – $1B
  - **2020**: $100M – $250M
  - **2021**: < $100 Decision Point

**Risk-focused IT Examinations with Critical Security Control Emphasis**

- **Pilot**
- **Implement**

**Progress Towards Maturity Target**

- **2018 – 2022**: Progress towards Maturity Target

**Transparent Accountability**

- **2018 – 2022**: Transparent Accountability

**Continual Improvement**

- **2018 – 2022**: Continual Improvement

**High Risk Scoping Proof of Concept**

- **2018 – 2019**: [“High Risk” Scoping Proof of Concept]
Automated Cybersecurity Examination Toolbox (ACET) Maturity Assessments

**Note:** Enhancement of ACET with Idaho National Labs (INL) based on the DHS Cyber Security Evaluation Tool (CSET) will be offered to industry via ncua.gov in 2020
## Training, Education, & Awareness (TEA) – Current Evolution

### New Examiners STEP
- **STEP 9**: Risk-Focused Examination Process (#119)
- **eLearning**: Information Technology for Examiners (#125)

### CORE Technical
- Cybersecurity – C Examiner Training Series (Cyber-C) eLearning Plan
- Cybersecurity Examination Process (#227)
- LearnCenter – Information Technology, BSA/AML, Payments, etc

### Subject Matter Examiner (SME)
- ISACA CSX Cybersecurity Fundamentals Workshop (#361)
- IT SME OJT (#254)
- IT SME Forum (#704)
- LearnCenter – Information Technology, BSA/AML, Payments, etc

### National and Regional Information Systems Officers
- LearnCenter – Information Technology, BSA/AML, Payments, etc

### Industry and Agency Conferences
- FIS Regulatory University - Information Technology, BSA/AML, Payments, etc.
- FFIEC/FDIC - Information Technology, BSA/AML, Payments, etc.
- Professional Designations and External Conferences
  - FFIEC IT Conference
National Initiative for Cybersecurity Education (NICE)

NIST SP 800-181 National Cybersecurity Workforce Framework (NCWF)

Workforce Categories
- Securely Provision
  - Risk Management
  - Software Development
  - Systems Architecture
  - Technology R&D
  - Systems Requirements Planning
  - Test & Evaluation
  - Systems Development

- Operate & Maintain
  - Data Administration
  - Knowledge Management
  - Customer Service & Tech Support
  - Network Services
  - Systems Administration
  - Systems Analysis

- Oversee & Govern
  - Legal Advice & Advocacy
  - Training Education and Awareness
  - Cybersecurity Management
  - Strategic Planning & Policy
  - Executive Cyber Leadership
  - Program/Project Management & Acquisition

- Protect & Defend
  - Cybersecurity Defense Analysis
  - Cybersecurity Defense Infr Analysis
  - Incident Response
  - Vulnerability Assessment & Management
  - Executive Cyber Leadership
  - Program/Project Management & Acquisition

- Analyze
  - Threat Analysis
  - Exploitation Analysis
  - All-Source Analysis
  - Targets
  - Language Analysis

- Collect & Operate
  - Collection Operations
  - Cyber Operations Planning
  - Cyber Operations

- Investigate
  - Cyber Investigation
  - Digital Forensics

Organizes Work Roles into Categories & Specialty Areas
Defines Knowledge Skills Abilities (KSAs)
Associates Tasks

Note: Due diligence with additional resources e.g. contracts, service level agreements, Key performance indicators (KPI), key risk indicators (KRI)
Cybersecurity Resources

NCUA recognizes the importance of cybersecurity and using the web safely and securely.

The information on this page is offered as resources for research and informational purposes. It may not reflect all of the requirements or guidance in this area and should not be construed as requirements except as noted. The NCUA does not endorse any vendor, service, or product.

When you access the links below, you might leave the NCUA's site.

Note: Recent example in the pending State Cybercrime resource list
Establish Cybersecurity Coordination
Working Group Under
- Enterprise Risk Management Committee (ERMC) and/or
- Cybersecurity Steering Committee (CSSC)
Office of Examination & Insurance (E&I)

NCUA BOARD MEETING – OCTOBER 2019