Mobile Malware & the Financial Sector
CYBERSECURITY AND THE FINANCIAL SYSTEM

THE FINCYBER STRATEGY PROJECT

THE STRATEGY REPORT

CYBERSECURITY WORKFORCE

CAPACITY-BUILDING TOOL BOX

CYBERSECURITY AND FINANCIAL INCLUSION

G20 NORMS PROPOSAL

TIMELINE OF CYBER INCIDENTS

RESEARCH WORKING PAPER SERIES

MONTHLY NEWSLETTER ‘FINCYBER’
Timeline of Cyber Incidents Involving the Financial Sector, 2007-Present

Filters:
- Region / Country
- Incident type
- Actor type
- Attribution
- Year

Data provided by the Cyber Threat Intelligence Unit of BAE Systems
Case Study #1: Ugandan Mobile Money Attack

Ugandan Mobile Money Hack
October 3

TARGET
Location: Uganda
Date Breach First Reported: October 5

INCIDENT
Method: SIM Card Fraud
Type: Theft

ACTOR:
Type: Non-State Actor
Attribution: Speculated

DESCRIPTION
Case Study #2: Liberia Mirai Botnet Attack

Liberia Mirai Botnet Attack
October 31

TARGET
Location: Liberia
Date Breach First Reported: November 4

INCIDENT
Method: DDoS
Type: Disruption

ACTOR:
Type: Non-State Actor
Attribution: High confidence

DESCRIPTION
THE SIX STRATEGIC PRIORITIES OF THE FINCYBER STRATEGY

Figure 2: Strategic Framework and Relationship Among Strategic Priorities

1. Cyber Resilience (deterrence by denial)
2. International Norms (deterrence by normative taboos)
3. Collective Response (deterrence by cost imposition)
4. Workforce
5. Capacity-Building
6. Digital Transformation/Financial Inclusion

Overarching Recommendations
CYBERSECURITY AND THE FINANCIAL SYSTEM

- The Fincyber Strategy Project
- Capacity-Building Toolbox
- Timeline of Cyber Incidents
- The Strategy Report
- Cybersecurity and Financial Inclusion
- Research Working Paper Series
- Cybersecurity Workforce
- G20 Norms Proposal
- Monthly Newsletter ‘Fincyber’
Cyber Resilience and Financial Organizations: A Capacity-building Tool Box

- **Board-Level Guide and Checklist**
  - Cybersecurity Leadership

- **CEO-Level Guide and Checklist**
  - Cybersecurity Leadership

- **CISO-Level Guide and Checklist**
  - Protecting the Organization

- **CISO-Level Guide and Checklist**
  - Protecting Customers

- **CISO-Level Guide and Checklist**
  - Protecting Connections to Third Parties

- **Guide and Checklist**
  - Incident Response

- **Guide and Checklist**
  - Ransomware: Prevention and Protection

- **Guide and Checklist**
  - Workforce Development
Cyber Resilience and Financial Organizations: A Capacity-building Tool Box

- Board-level guide and checklist: Cybersecurity leadership
- CEO-level guide and checklist: Cybersecurity leadership
- CISO-level guide and checklist: Protecting the organization
- CISO-level guide and checklist: Protecting customers
- CISO-level guide and checklist: Protecting connections to third parties
- Guide and checklist: Incident response
- Guide and checklist: Ransomware: prevention and protection
- Guide and checklist: Workforce development

Languages: English, Arabic, Dutch, French, Portuguese, Russian, Spanish, Hindi, Japanese, Mandarin
RANSOMWARE: PREVENTION AND PROTECTION

REAL-TIME PROTECTION

Ransomware is a growing threat since malicious actors have found ways to monetize malware paralyzing computer systems and demanding a ransom be paid for their release. Unlike other malware, which often has to stay hidden for long periods of time to operate effectively, ransomware is engineered to execute quickly through spear-phishing, compromised websites, and corrupted downloads. Financial institutions are particularly vulnerable to the impact of ransomware because these attacks can threaten the ability to move funds quickly and efficiently and because they are considered lucrative targets. However, bad actors sometimes break their promises; even after a ransom is paid, some attackers do not remove the malware or release confidential data.

- Invest in anti-malware protection systems that adapt to new threat intelligence in real-time.
- Evaluate the security of all devices connected to networks that house sensitive or essential information. Connect all nonessential systems to a separate network.
  - Be particularly careful when bringing IoT or "smart devices" into your workspaces, since these systems often have weaker or nonexistent security systems and can be targeted as access points to essential systems.
  - Consider the security of remote work setups. Ensure security tools work off-network to monitor all web traffic.
  - Promote employee education around phishing attacks and the necessity of strong password protections.
- Consider implementing multifactor authentication across your organization if feasible.
- Keep all systems and software regularly updated. Change settings to allow for automated updates if possible.
- Develop an incident response and crisis management plan for how to deal with a ransomware attack and the loss of valuable data.
- Prepare an external communication plan in the event of a ransomware attack.

DATA BACKUPS

- Invest in secure, regularly updated backup systems that keep your data protected.
  - If using USBs or hard drives, physically disconnect these devices from networked computers after backups are finished.
  - If using cloud storage, equip server with high-level encryption and multifactor authentication.
- Create a read-only copy of the general ledger for worst case disaster recovery.
- Develop systems that perform automated data recovery and remediation.
- Develop scenarios to assess how long it will take to recover critical data and business services.

REGULATORY ENVIRONMENT

- Evaluate the relevant regulatory and legal guidance for ransomware in your operating environment.
  - Consider country-specific guidance. Develop a plan for periodic evaluation of changing guidance.
  - Consider financial-sector specific guidance.
  - Consider international legal and regulatory requirements.
- Assess risks involved with paying a ransom. In some cases, paying a ransom could violate existing sanctions regimes in place against hostile actors.
- Liaison with local law enforcement. Build connections for quick information sharing in the event of an attack.
- Assess the benefits and drawbacks of cyber insurance policies for ransomware.

Gauging Your Organization’s Ransomware Readiness

Consider the following questions when developing a ransomware prevention and protection plan.

1. Does your organization have regularly scheduled backups?
   - Are these backups disconnected from your network, either via cloud storage systems or air-gapped USBs/hard drives?

2. Are any nonessential devices connected to your organization’s network?
   - Can they be moved to other networks that do not house sensitive data?

3. Does your organization understand the regulatory and legal risks involved with paying a ransom?
   - Legal guidance on this varies from country to country and is frequently updated.

4. Does your organization regularly update its software and systems? Are updates automated?

5. Does your organization have a plan for how to deal with a ransomware attack and the loss of valuable data?

6. Does your organization have a cyber insurance policy? If so, how does that plan cover ransomware attacks?
   - Some plans explicitly prohibit ransom payments, while others will cover such a payment as part of the policy.
• Gauging Your Organization’s Ransomware Readiness

• Real-Time Protection

• Data Backups

• Regulatory Environment
**Ransomware Checklist**

**Ransomware Readiness**
- As you develop a ransomware prevention and protection plan, periodically assess the following:
  - Does your organization have regular scheduled backups?
  - Are any nonessential devices connected to your organization's network?
  - Does your organization understand the regulatory and legal risks involved with paying a ransom?
- Does your organization regularly update its software systems? Are these updates automated?
- Does your organization have policies for dealing with a ransomware attack and data loss?
- Does your organization have a cyber insurance policy? If so, how does that plan cover ransomware attacks?

**Real-Time Protection**
- Invest in anti-malware protection systems that adapt to new threat intelligence in real-time.
- Evaluate the security of all devices connected to networks that house sensitive or essential information.
  - Connect all nonessential systems to a separate network.
  - Consider the security of remote work setups. Ensure security tools work off-network to monitor all web traffic.
  - Promote employee education around phishing attacks and the necessity of strong password protections.
- Consider implementing multi-factor authentication across your organization if feasible.
- Keep your software and systems regularly updated.
- Change settings to allow for automated updates if possible.
- Develop an incident response and crisis management plan to deal with a ransomware attack and the loss of valuable data.
- Prepare an incident communication plan in the event of a ransomware attack.

**Data Backups**
- Invest in secure, regularly-updated backup systems that keep your data protected.
  - If using USBs or external drives, physically disconnect these devices from networked computers after backups are complete.
  - If using cloud storage, ensure recovery with high-level encryption and multi-factor authentication.
- Create a read-only copy of the general ledger for worst-case disaster recovery.
- Develop systems that perform automated data recovery and remediation.
- Develop scenarios to assess how long it will take to recover critical data and business services.
REAL-TIME PROTECTION

☐ Invest in anti-malware protection systems that adapt to new threat intelligence in real-time.

☐ Evaluate the security of all devices connected to networks that house sensitive or essential information.
   - Connect all nonessential systems to a separate network.
   - Consider the security of remote work setups. Ensure security tools work off-network to monitor all web traffic.

☐ Promote employee education around phishing attacks and the necessity of strong password protections.

☐ Consider implementing multifactor authentication across your organization if feasible.

☐ Keep all software and systems regularly updated.
   - Change settings to allow for automated updates if possible.

☐ Develop an incident response and crisis management plan for how to deal with a ransomware attack and the loss of valuable data.
   - Prepare an external communication plan in the event of a ransomware attack.
Next Steps: Turning Words Into Action

CURRENT CARNEGIE WORK

FinCyber Strategy Report
Launched July 2020
Published November 2020

Six Strategic Priorities

<table>
<thead>
<tr>
<th>Cyber Resilience</th>
<th>Norms</th>
<th>Collective Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workforce</td>
<td>Capacity-Building</td>
<td>Financial Inclusion</td>
</tr>
</tbody>
</table>

December 2020
Co-hosted with IMF, WB, WEF

TOOL BOX UPDATE DECEMBER 2020

FUTURE CARNEGIE WORK

CyberFI Working Group Process

- Policy and Research Advisory Group
- Regional Implementation Center Group

Tool Box Update 2021

GFCE Cybil Portal
Research Agenda
Annotated Bibliography
Research Paper Series

December 2021 Conference
Carnegie's monthly newsletter for policymakers and industry leaders, highlighting key cybersecurity trends and insights affecting the global financial system.