CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

THE GLOBAL THINK TANK

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

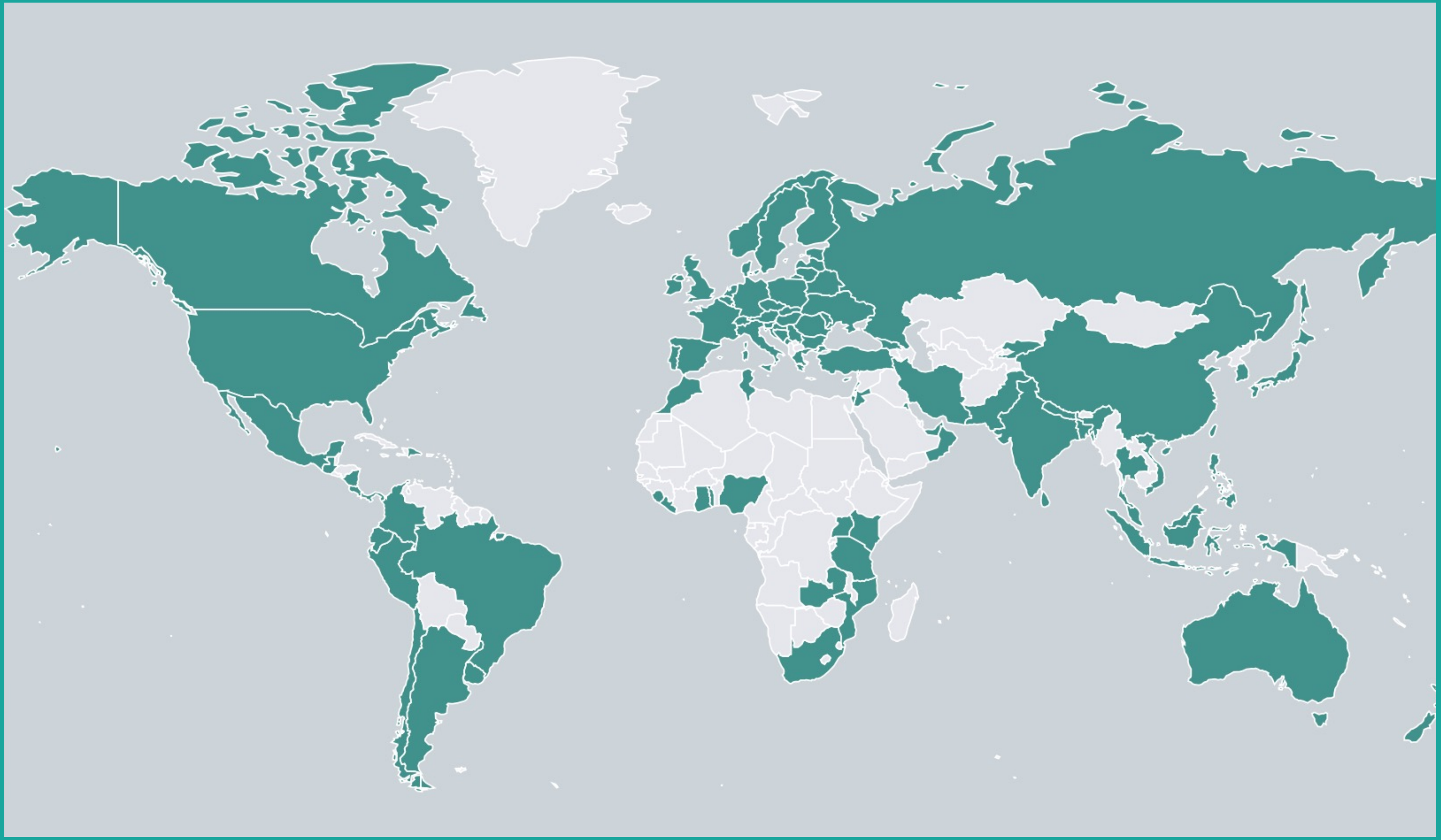
G20 NORMS PROPOSAL

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

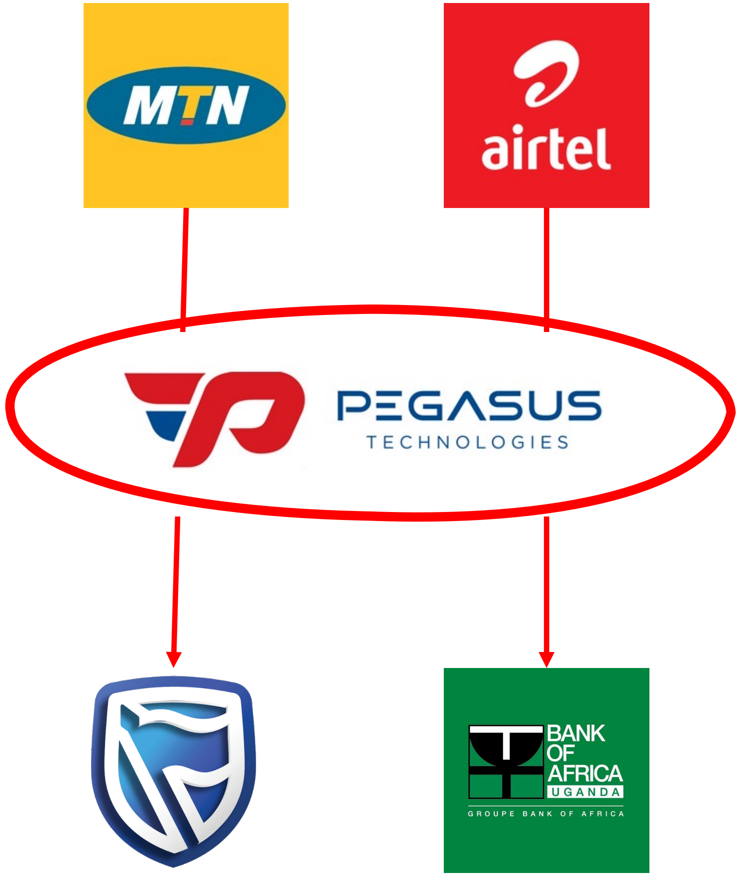
Actor type

Attribution

Year

Data provided by the Cyber Threat Intelligence Unit of BAE Systems

Case Study #1: Ugandan Mobile Money Attack



2020

Ugandan Mobile Money Hack
October 3

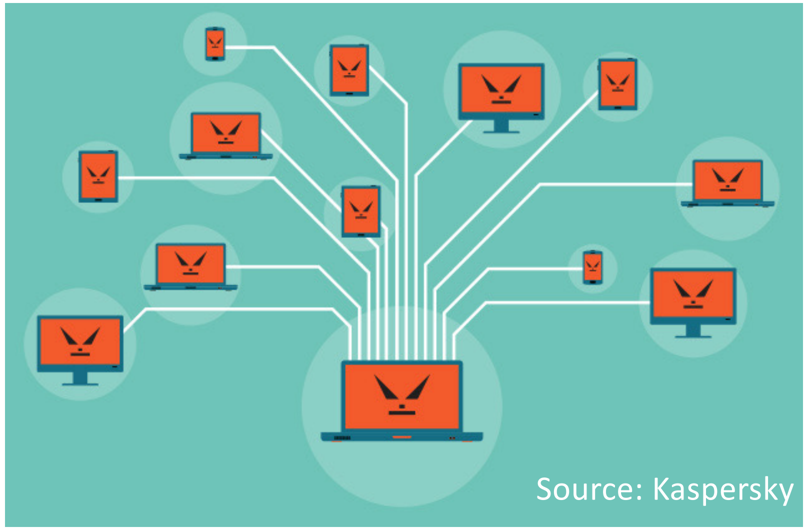
TARGET
Location: Uganda
Date Breach First Reported: October 5

INCIDENT
Method: SIM Card Fraud
Type: Theft

ACTOR:
Type: Non-State Actor
Attribution: Speculated

DESCRIPTION

Case Study #2: Liberia Mirai Botnet Attack



Source: Kaspersky

2016

Liberia Mirai Botnet Attack
October 31

TARGET
Location: Liberia
Date Breach First Reported: November 4

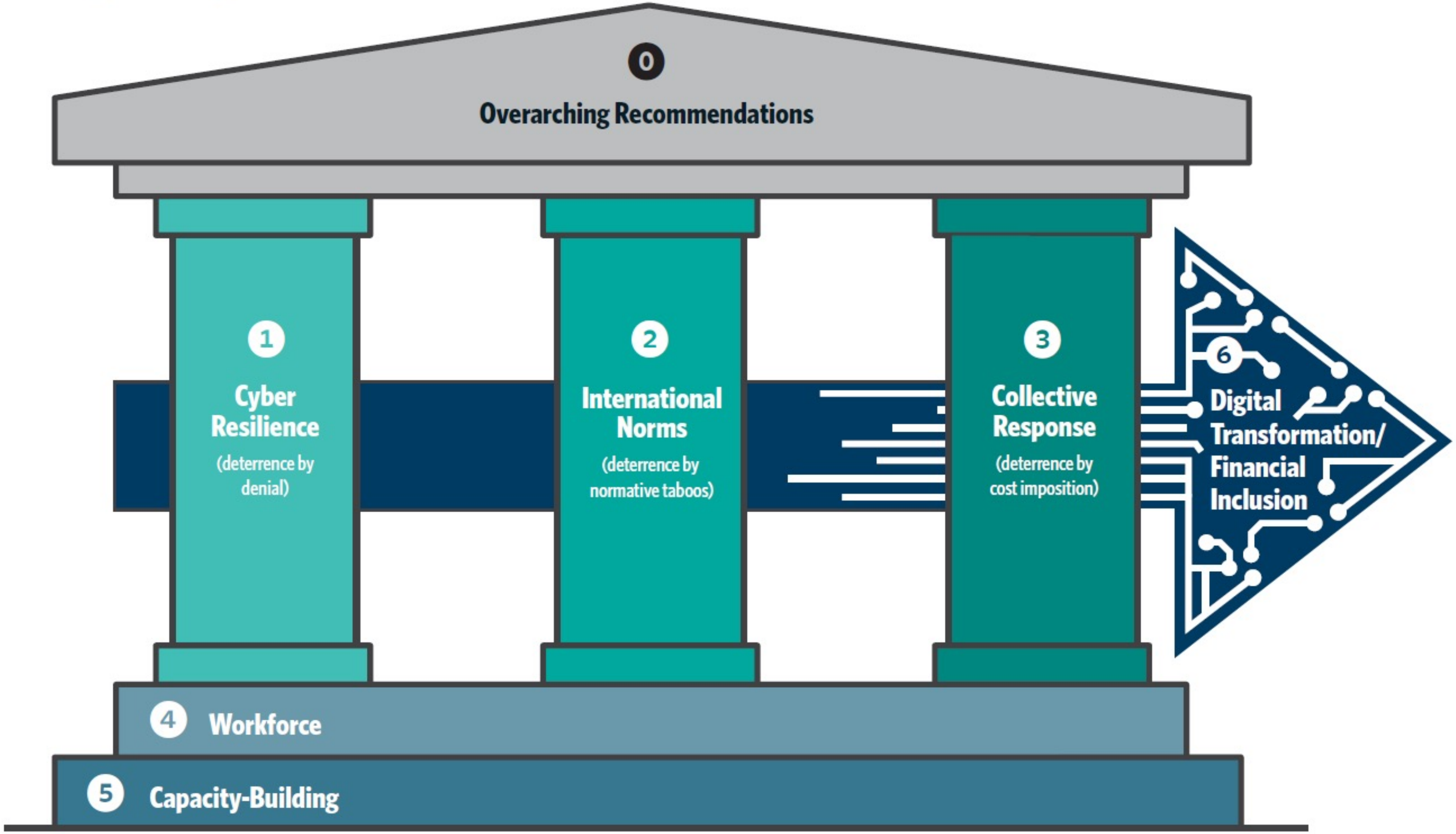
INCIDENT
Method: DDoS
Type: Disruption

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


0
Overarching Recommendations
1
Cyber Resilience
(deterrence by denial)
2
International Norms
(deterrence by normative taboos)
3
Collective Response
(deterrence by cost imposition)
6
Digital Transformation/ Financial Inclusion
4
Workforce
5
Capacity-Building

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'

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

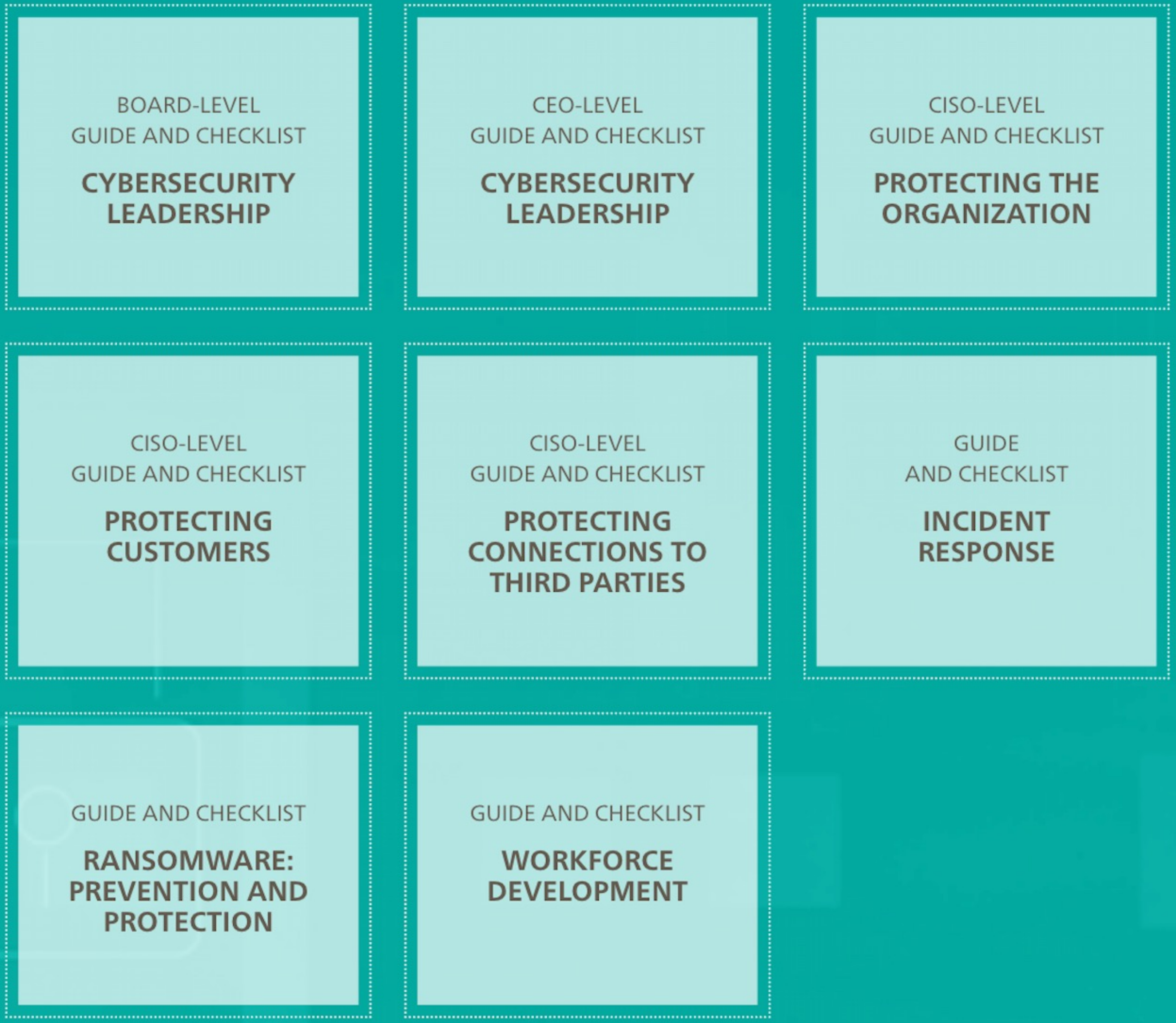
GUIDE AND CHECKLIST

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.

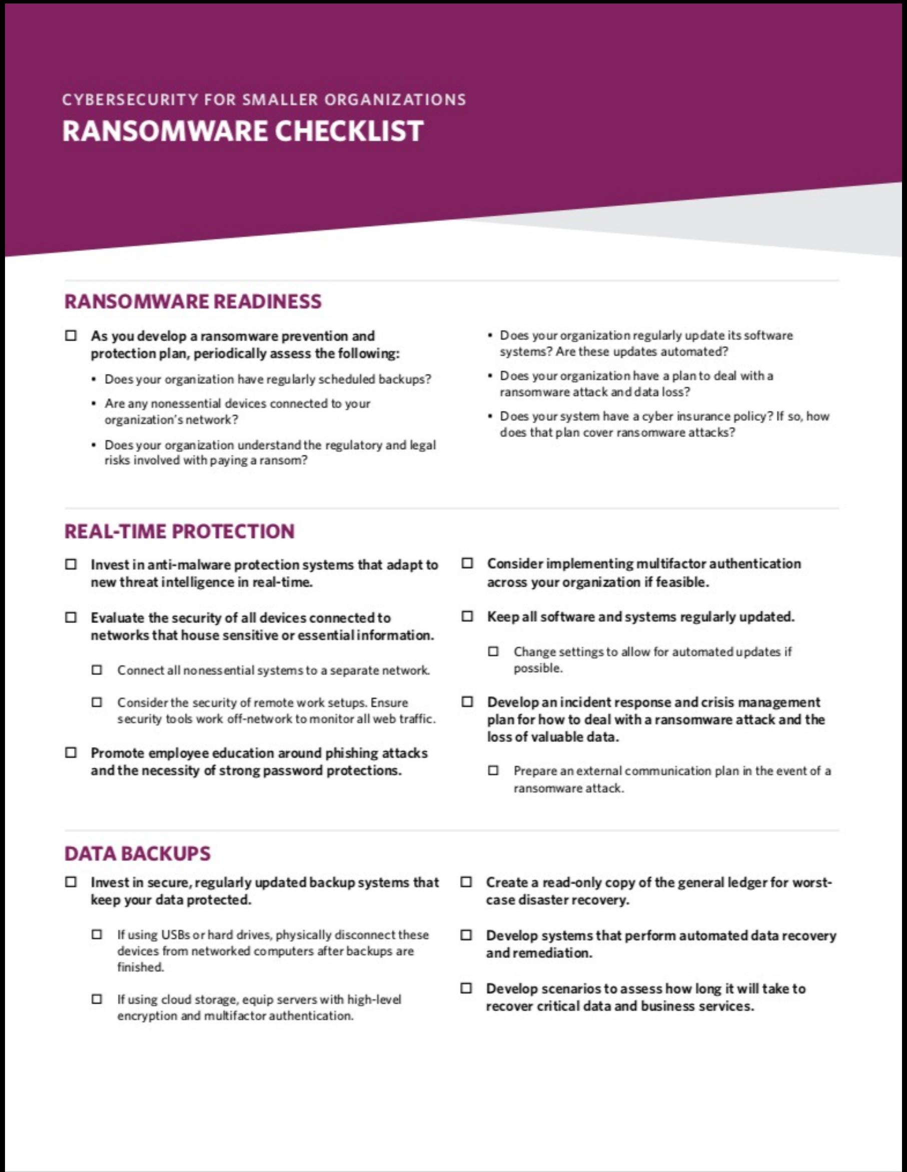
Gauging Your Organization's Ransomware Readiness

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.

RANSOMWARE: PREVENTION AND PROTECTION

- Gauging Your Organization’s Ransomware Readiness
- Real-Time Protection
- Data Backups
- Regulatory Environment



CYBERSECURITY FOR SMALLER ORGANIZATIONS

RANSOMWARE CHECKLIST

RANSOMWARE READINESS

□ **As you develop a ransomware prevention and protection plan, periodically assess the following:**

- Does your organization have regularly 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 a plan to deal with a ransomware attack and data loss?
- Does your system 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 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.

DATA BACKUPS

□ **Invest in secure, regularly updated backup systems that keep your data protected.**

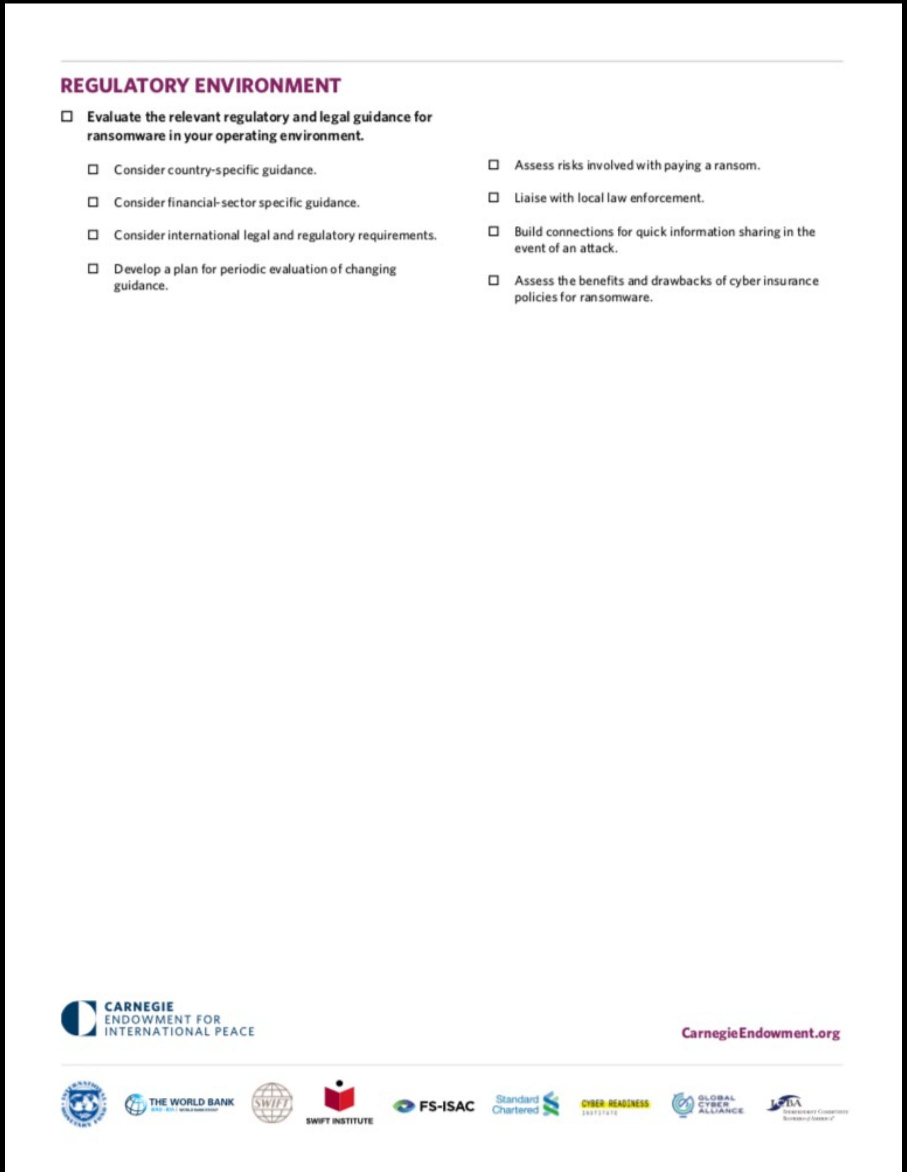
  □ If using USBs or hard drives, physically disconnect these devices from networked computers after backups are finished.

  □ If using cloud storage, equip servers 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.

  □ Consider financial-sector specific guidance.

  □ Consider international legal and regulatory requirements.

  □ Develop a plan for periodic evaluation of changing guidance.

  □ Assess risks involved with paying a ransom.

  □ Liaise 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.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org

CYBERSECURITY FOR SMALLER ORGANIZATIONS

RANSOMWARE CHECKLIST

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.

Official Partners

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

INTERNATIONAL MONETARY FUND

SWIFT

SWIFT INSTITUTE

FS-ISAC

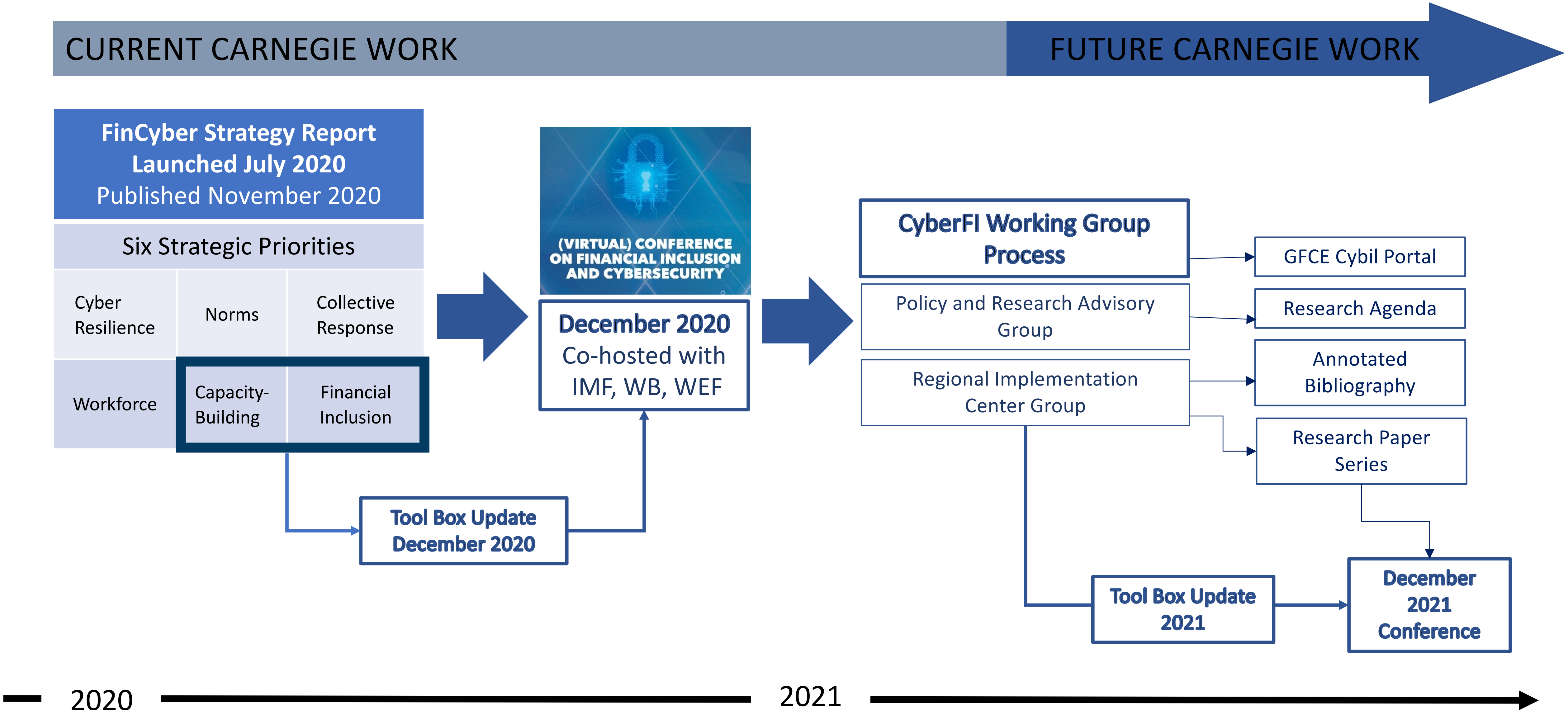
Standard Chartered

CYBER READINESS INSTITUTE

GLOBAL CYBER ALLIANCE.

ICBA
Independent Community Bankers *of* America®

Next Steps: Turning Words Into Action



CURRENT CARNEGIE WORK

FUTURE CARNEGIE WORK

FinCyber Strategy Report Launched July 2020
Published November 2020

Six Strategic Priorities

Cyber Resilience	Norms	Collective Response
Workforce	Capacity-Building	Financial Inclusion

Tool Box Update December 2020

(VIRTUAL) CONFERENCE ON FINANCIAL INCLUSION AND CYBERSECURITY

December 2020
Co-hosted with IMF, WB, WEF

CyberFI Working Group Process

Policy and Research Advisory Group

Regional Implementation Center Group

GFCE Cybil Portal

Research Agenda

Annotated Bibliography

Research Paper Series

Tool Box Update 2021

December 2021 Conference

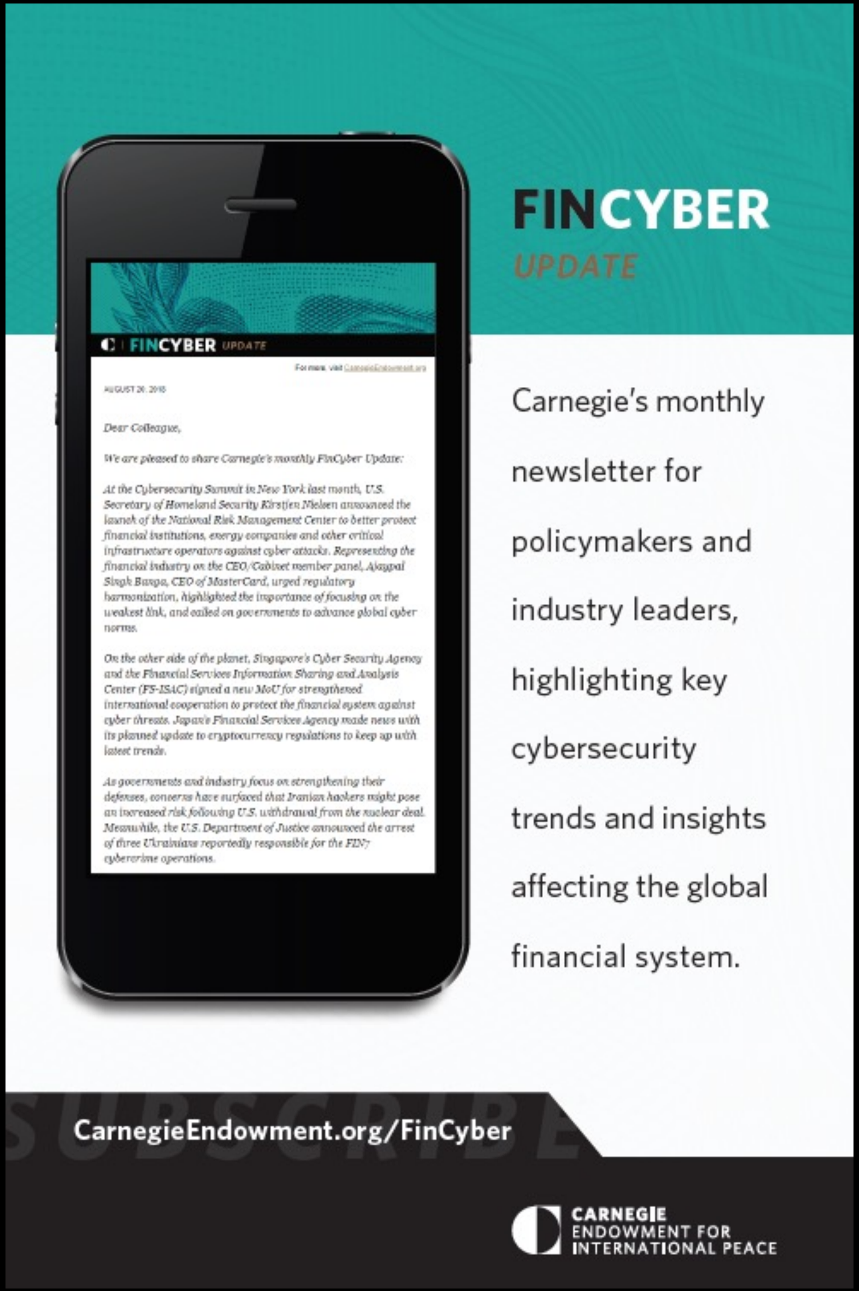
2020

2021

WWW.CARNEGIEENDOWMENT.ORG/FINCYBER

taylor.grossman@ceip.org

@tgrossman_



FINCYBER UPDATE

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

FINCYBER UPDATE

For more, visit CarnegieEndowment.org

AUGUST 20, 2018

Dear Colleague,

We are pleased to share Carnegie's monthly FinCyber Update:

At the Cybersecurity Summit in New York last month, U.S. Secretary of Homeland Security Kirstjen Nielsen announced the launch of the National Risk Management Center to better protect financial institutions, energy companies and other critical infrastructure operators against cyber attacks. Representing the financial industry on the CEO/Cabinet member panel, Ajaypal Singh Banga, CEO of MasterCard, urged regulatory harmonization, highlighted the importance of focusing on the weakest link, and called on governments to advance global cyber norms.

On the other side of the planet, Singapore's Cyber Security Agency and the Financial Services Information Sharing and Analysis Center (FS-ISAC) signed a new MoU for strengthened international cooperation to protect the financial system against cyber threats. Japan's Financial Services Agency made news with its planned update to cryptocurrency regulations to keep up with latest trends.

As governments and industry focus on strengthening their defenses, concerns have surfaced that Iranian hackers might pose an increased risk following U.S. withdrawal from the nuclear deal. Meanwhile, the U.S. Department of Justice announced the arrest of three Ukrainians reportedly responsible for the FIN7 cybercrime operations.

CarnegieEndowment.org/FinCyber

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE