FPP 2021 Cyber Safety Virtual Forum:
The Undeniable Link Between Cyber Safety and Financial Capability

Tuesday, September 28, 2021
1:00 p.m. – 3:30 p.m. Eastern
Pursue the Certified Practitioner In Financial Capability

CPFinCAP

CPFinCap.org

ELEVATING FINANCIAL CAPABILITY FOR ALL
FPP 2021 Coalition Regional Roundtables

“Taking a Seat at the Table: Conversations to Elevate Financial Diversity, Equity and Inclusion”

September 30 – December 10, 2021
Live and Virtual Sessions

South Florida (Live, In Person):
Broward and Palm Beach Counties

Thursday, September 30, 2021
9:00 a.m.—12:00 noon
City of Lauderhill City Hall Commission Chamber
5581 W. Oakland Park Blvd.
Lauderhill, FL 33313

To Register:
https://FPPCoalition.org/event/rr0930
Meet Today’s Guest Experts

The Undeniable **Link** Between Cyber Safety and Financial Capability
Today's Virtual Forum Format:
- 10-minute TedX-Style Talk
- 10-minute Small Group Breakout Conversation
- 10-minute Debrief of Conversation
John Raymond, Jr.
Vice President, Information Security
Suncoast Credit Union

“Ransomware Protection and Response”

The Undeniable Link Between Cyber Safety and Financial Capability
FLORIDA PROSPERITY PARTNERSHIP
2021 CYBER SAFETY VIRTUAL FORUM

RANSOMWARE PROTECTION & RESPONSE

JOHN RAYMOND
VP, INFORMATION SECURITY
SUNCOAST CREDIT UNION
WHAT IS IT & WHY SHOULD I BE CONCERNED

Ransomware is a form of malware used to encrypt files on a victim's systems

- Threat actor normally demands a ransom in order to restore access to the encrypted files.
- Ransom demands are time limited – failure to pay during the timeframe identified may increase the ransomware payment demands.

Half of organizations surveyed were hit with ransomware in 2020

- Size doesn’t matter – Ransomware attacks can be targeted or crimes of opportunity
- 73% of attacks resulted in data being encrypted

SOURCE: STATE OF RANSOMWARE 2020 REPORT - SOPHOS
WHAT ARE THE COSTS?

- Average ransomware payments in 2020 was $312K.
- The largest payment doubled from $5m to $10m with the largest demand being $30m.

Average U.S. cost of ransomware remediation was $622K

- Cost to recover does not include ransomware payment
- Only 64% of organizations have cyber insurance policies that cover ransomware
- 94% of ransomware incidents are paid through cyber insurance

SOURCE: STATE OF RANSOMWARE 2020 REPORT - SOPHOS
## How Ransomware Infects Systems

<table>
<thead>
<tr>
<th>How it was delivered</th>
<th>Number of Incidents in 2020</th>
<th>Percentage of Incidents in 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>File download/email with malicious link</td>
<td>741</td>
<td>29%</td>
</tr>
<tr>
<td>Remote attack on server</td>
<td>543</td>
<td>21%</td>
</tr>
<tr>
<td>Email with malicious attachment</td>
<td>401</td>
<td>16%</td>
</tr>
<tr>
<td>Misconfigured public cloud</td>
<td>233</td>
<td>9%</td>
</tr>
<tr>
<td>Remote Desktop Protocol (RDP)</td>
<td>221</td>
<td>9%</td>
</tr>
<tr>
<td>3rd party supplier</td>
<td>218</td>
<td>9%</td>
</tr>
<tr>
<td>USB/Removable Media Device</td>
<td>172</td>
<td>7%</td>
</tr>
</tbody>
</table>

*Source: State of Ransomware 2020 Report - Sophos*
Assume you’re going to be breached - Develop a formal incident response plan.

- Assign responsibilities and develop a strategy for recovery w/feedback from GRC team
- Align your incident response program w/NIST to include the following phases:
  - Preparation, Detection, Analysis, Containment, Eradication, Recovery and Post Incident Review
  - Include key organizational functions in your incident response team
  - Senior Leadership, Legal, Compliance, Marketing, Risk Management, IT, Info Security
- Develop playbooks for specific incident types
- Ensure your insurance carrier reviews your incident plan

Develop a communication plan

- Determine how and what will be shared
- Be prepared to communicate out of band

Keep applications and operating systems patched up to date

- Many ransomware attacks take advantage of existing vulnerabilities to infect systems

Invest in endpoint protection software designed to prevent ransomware

- Next generation endpoint security tools can prevent ransomware attacks and roll systems back to a safe condition

Protect your data on premise and in the cloud

- Segment your networks and limit access to only what’s required
- Encrypt sensitive information such as PII & PCI data

Regularly backup your systems. Store backups offsite and offline

- New threat actor tactics steal your data while encrypting it. Backups will not help with data loss

SOURCE: STATE OF RANSOMWARE 2020 REPORT - SOPHOS
### PROTECTING MY ORGANIZATION

#### Implement Multi-factor authentication
- Helps prevent ransomware attacks and various other cyberattacks
- Consider MFA for all user accounts
- Require MFA for all admin accounts

#### Implement email controls
- Add layers of security to protect against ransomware
  - Email sandboxing
  - Implement SPF, DKIM, and DMARC
- Email sandboxing
- Implement SPF, DKIM, and DMARC

#### Egress firewall traffic
- Examine all outbound traffic and implement geolocation blocking to locations you don’t do business with
- Inspect outbound TLS traffic for unauthorized transmission of PII and PCI data

#### Security Awareness Training
- Staff are your first line of defense
- Encourage safe cyber hygiene
  - Educate them to recognize phishing attacks
  - Don’t download content from untrusted sites
  - Don’t connect unauthorized equipment such as USBs.

#### Prioritize your critical systems & be prepared to take them offline
- Authorize your incident response commander to take critical systems offline under very short notice

#### Ensure your cyber insurance policy covers ransomware
- 94% of ransomware incidents are paid for by cyber insurance – make sure you’re covered!

**SOURCE:** STATE OF RANSOMWARE 2020 REPORT - SOPHOS
Detect & Analyze

• Detect and stop all attacks in progress
• Shut down critical systems to prevent further infection
• Analyze the Who, What, Why, When, Where and How of the incident
• Begin documenting incident & notify your insurance carrier
• Capture the ransomware demand
• Share with your insurance carrier
• Share with forensics team assigned by carrier

Contain

• Keep devices powered on but disconnected from the network
• Isolate backups and backup servers
• Isolate impacted systems & networks
• Disable all remote & internet access
• Disable inbound and outbound internet access for all systems
• Disable internal Remote Desktop Protocol access
• Collect evidence and logs
• Reset passwords for all accounts

Eradicate

• Work with your assigned forensic team to eradicate and remediate the incident

Do Not

• Do not reimage systems until instructed to do so by the forensic team
RESOURCES

StopRansomware.gov

DHS Ransomware Guide

Cyber Incident Response Playbook Sample

Ransomware Playbook Sample

State of Ransomware 2020 Report - Sophos
If your organization was hit with ransomware, what would be the impact to the organization and the people you serve?
If your organization was hit with ransomware, what would the impact be to the organization and the people you serve?
Sarah deBoer-Hjort
President
Necessities for Children
“Cyber Safety and Opportunities for Youth”

The Undeniable Link Between Cyber Safety and Financial Capability
Our mission is to provide support to underserved and minority youth; empowering and equipping them with 21st century skills & tools to succeed. We change the trajectory of lives through the power of education.

www.necessitiesforchildren.org
1451 W. Cypress Creek Rd, Suite 300 Fort Lauderdale, FL 33309
CYBER SAFETY & CYBERSECURITY

→ STRANGER DANGER

→ CYBERSECURITY CAREER OPPORTUNITIES!
YOUR DIGITAL FOOTPRINT IS JUST AS IMPORTANT AS YOUR ACTUAL FOOTPRINT.
CYBERSECURITY
A CAREER OPPORTUNITY

➔ Problem Solving
➔ Job Growth / Career Outlook
➔ Salary
➔ Helping People
➔ Variety

TIP: Go for an internship or summer job in technology or cybersecurity. Many companies and governments hire those people first!
A cyber privacy parable

Protect Yourself, Your Family and Friends. Be Safe Online!

E: director@necessitiesforchildren.org
P: 954-246-0602

NFC Necessities for Children
What specific examples have you encountered, from your own personal experience or when serving others, where a person became a victim of a cybercrime?
Mark Batchelor
Vice President, Community-Based Programs
Cybercrime Support Network

“More Than Money: The True Cost of Cybercrime”

The Undeniable Link Between Cyber Safety and Financial Capability
More Than Money: The True Cost of Cybercrime

Mark Batchelor
Vice-President, Community Based Programs

Giving victims of cybercrime a voice.
IC3 by the Numbers

- Over 2,000 complaints received per day on average
- 5,679,259 complaints reported since inception ('00)
- $4.2 billion in victims' losses in 2020
- Over 440,000 complaints received per year on average (over last 5 years)
1 out of 4 U.S. adults are impacted by cybercrime

Actual losses could be **$420 billion** per year for 50M American consumers and SMBs.

Source: Gallop, 2019
#4 Total Losses Per State (+ $295 million)

#2 Number of Victims per State (53,793)

Source: FBI IC3 Annual Report 2020
Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

By Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber

Sept. 7, 2017

45% of US Population

The WannaCry ransomware attack has spread to 150 countries

New variations of the ransomware have begun to surface

By Andrew Liptak | @AndrewLiptak | May 14, 2017, 1:42pm EDT

$18.5 billion in fines alone

Target data theft affected 70 million customers

© 10 January 2014

Image descriptions: 3 news headlines (Equifax cyberattack affects 143 million in US, WannaCry ransomware attack has spread to 150 countries, Target data theft affects 70 million customers)
But how much do we really know about the effect on the individual?
Company shuts down because of ransomware, leaves 300 without jobs just before holidays

Company tells employees to seek new employment after suspending all operations right before Christmas.
Lost job  Lost wages  Unpaid bills
GOV’T IMPOSTER SCAMS
$175.16M Total Losses
$1,250 median loss

IRS IMPOSTER
$1,200 median loss

SOCIAL SECURITY
$1,853 median loss

MEDICARE/HEALTH
$500 median loss

Data as of June 30, 2021

Source: FTC Consumer Sentinel 2020
- Housing Insecurity
- Food Insecurity
- Medical Bills
- Credit Damage
More than just dollars lost...

...cybercrime impacts lives
Romance scams: when a criminal adopts a fake online identity to gain a victim’s affection and trust.

The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim. -FBI
Victimization Tactics

- Establishment of trust
- Isolation
  - Emotional
  - Interpersonal
  - Weakening of supports system
- Coercive Control
  - Monopolization
  - Economic abuse
  - Psychological Abuse
  - Fear
    - Physical threat
    - Abandonment
Depression (suicidal ideation)

Loss of property

Broken relationships

Substance abuse issues
CONVERSATION STARTER:

What are some of the consequences of cybercrime that may not be so obvious to us?
What are some of the consequences of cybercrime that may not be so obvious to many?
Patrick Craven
Director
Center for Cyber Safety and Education

“Keeping Your Children and Family Safe Online”

The Undeniable Link Between Cyber Safety and Financial Capability
"Making the Cyber World a Safer Place for Everyone"

PATRICK CRAVEN
Director
center@isc2.org
WHO WE ARE:

Nonprofit charity of (ISC)²

Cyber Safety Education
- Children, Parents and Senior Citizens
- Developed by Cybersecurity Professionals

Scholarships
- High school, college, veterans, women and graduates
Scholarships

- Women
- Undergraduate
- Graduate
- Veterans
- High School
- Diversity

20201
- $230,000 awarded
- Over 1,100 applicants
- 70 students

2022 OPEN NOV 15

IAmCyberSafe.org/scholarships
40% Have Chatted with a Stranger Online

All children (n=170).

*Center’s Children’s Internet Usage Study
25% of those children gave a stranger their phone number.*

*Center’s Children’s Internet Usage Study
ONE-OUT-OF-FIVE actually spoke with a stranger.*

All children (n=170).
*Center’s Children’s Internet Usage Study
One-out-of-ten met a stranger in person.*

All children (n=170).

*Center’s Children’s Internet Usage Study
OVER 1/2

of the children surveyed are on the internet after 10pm on a school night, not doing homework.

All children answering (n=166)
*Center’s Children’s Internet Usage Study
JUST THE FACTS

10% admit they were late to school because of being online late at night.

All children answering (n=171)

*Center’s Children’s Internet Usage Study
JUST THE FACTS.

5% missed school because they were too tired from being online late.

All children answering (n=171)
*Center’s Children’s Internet Usage Study
GARFIELD'S Cyber Safety Adventures

- Children’s Internet Usage Study
- In partnership with (ISC)² and Paws, Inc.
- 20-30 minutes lessons
- Privacy, Safe Posting and Cyberbullying
- Age target 6-11
- FOUR Educational Awards
Educator Kit

• 30 Children
• Cartoon on USB Thumb Drive
• Trading Cards, Stickers, Posters and more!
• Letter for Parents
Safe and Secure Online

- Children (11-14), Teens, Parents and Senior Citizens
  - PowerPoints, Handouts, Videos
- In-person or VIRTUAL EVENTS
- Available in 24 languages
- Free at IAmCyberSafe.org/volunteers
- No Application or Forms
How to Volunteer like a Cybersecurity Professional

- IAmCyberSafe.org/volunteers
- In depth look at Children’s, Parents and Senior materials
- Overview of resources available to get started
- How to get started and have successful presentation
- Virtual volunteering
- Q&A
GET INVOLVED

1) Speaker:
   a) Schools
   b) Community & Senior Centers
   c) Public Libraries
   d) Virtual Presentations

2) Corporate and Chapter Give Back:
   ◦ Sponsor a Scholarship
   ◦ Adopt a School
   ◦ Support Community Events
Cyber Safety Day

One-day event to provide 3rd graders with Garfield's Cyber Safety Adventures

Joint effort between community leaders, local companies and schools

Creating awareness about internet safety while giving back
QUESTIONS?

center@isc2.org

IAmCyberSafe.org

Follow us on social media:

Center for Cyber Safety and Education
At what age should a child be given access to connected technology, phones and social media?
Pursue the Certified Practitioner In Financial Capability

CPFinCap.org
FPP 2021 Coalition Regional Roundtables

“Taking a Seat at the Table: Conversations to Elevate Financial Diversity, Equity and Inclusion”

September 30 – December 10, 2021
Live and Virtual Sessions
FPP 2021 Cyber Safety Virtual Forum:
The Undeniable Link Between Cyber Safety and Financial Capability

Tuesday, September 28, 2021
1:00 p.m. – 3:30 p.m. Eastern