# Cybersecurity Best Practices for Credit Unions

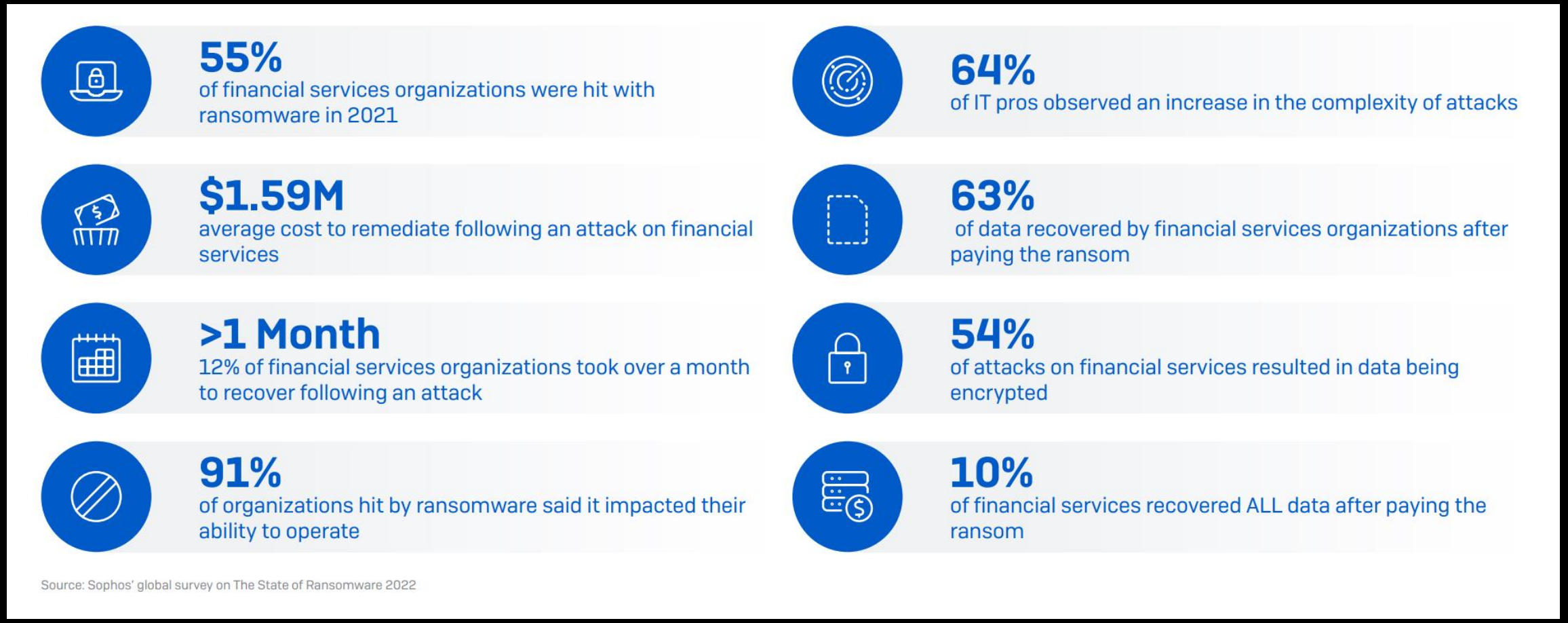
**Harry Santiago-Perez, CPA, CIA**
Business Advisory Director
**Josue Hill Felix**
Cybersecurity and Risk Management Senior Manager
**Wilfredo R Vera Pujols, CISA, CDPSE, MCS**
Cybersecurity and Risk Management Manager

# Agenda

- Current Cybersecurity Landscape
- Key Cybersecurity Threats
- Compliance and Regulatory Requirements
- Building a Cybersecurity Culture
- Best Practices & Recommendations


Employees can be an
organization’s biggest liability
when it comes to cybersecurity.

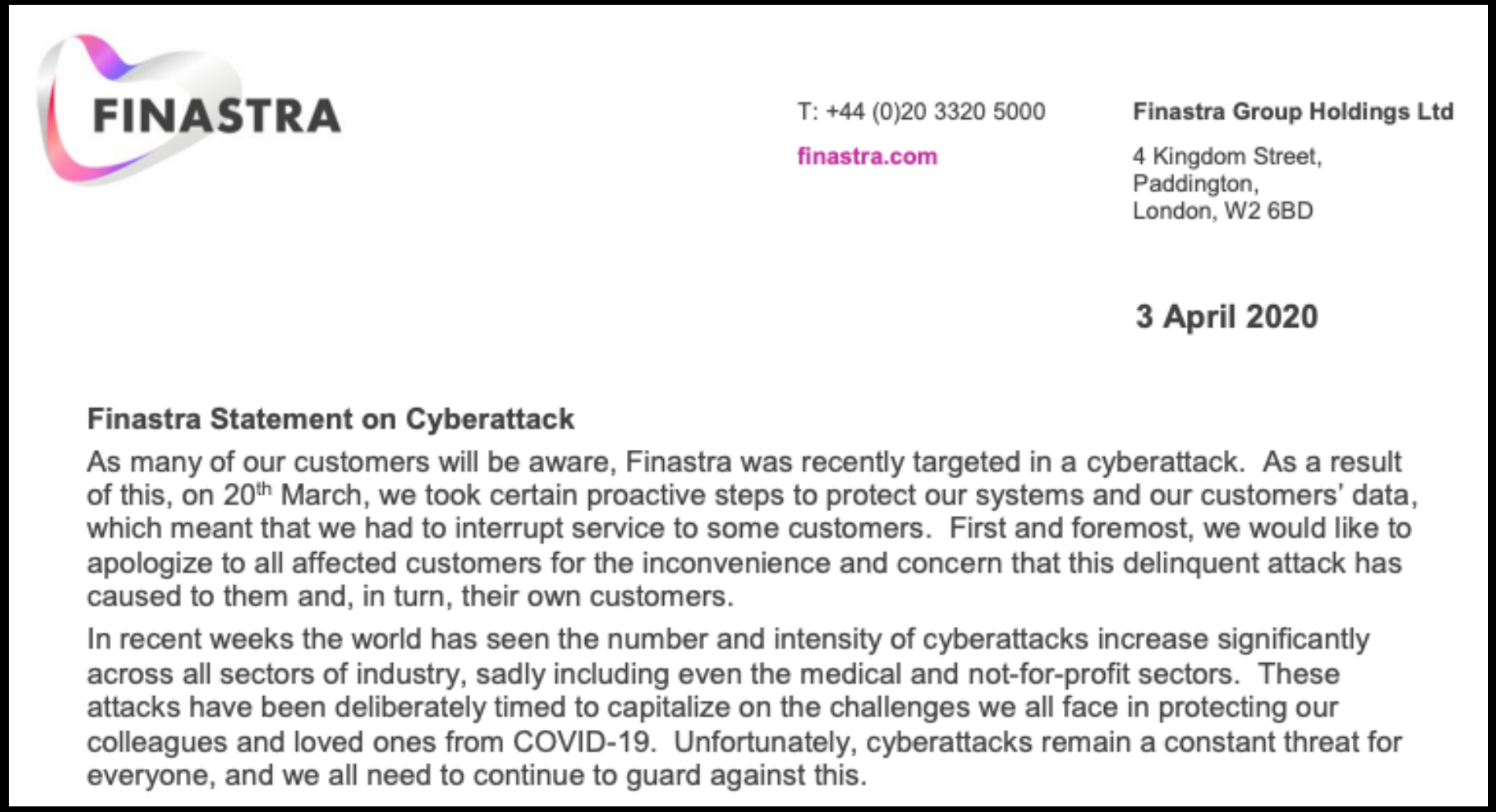
# Facts




Sophos
https://partnernews.sophos.com/

# Ramsomware

# Finastra Ransomware Attack



FINASTRA

T: +44 (0)20 3320 5000
finastra.com

**Finastra Group Holdings Ltd**
4 Kingdom Street,
Paddington,
London, W2 6BD

**3 April 2020**

**Finastra Statement on Cyberattack**

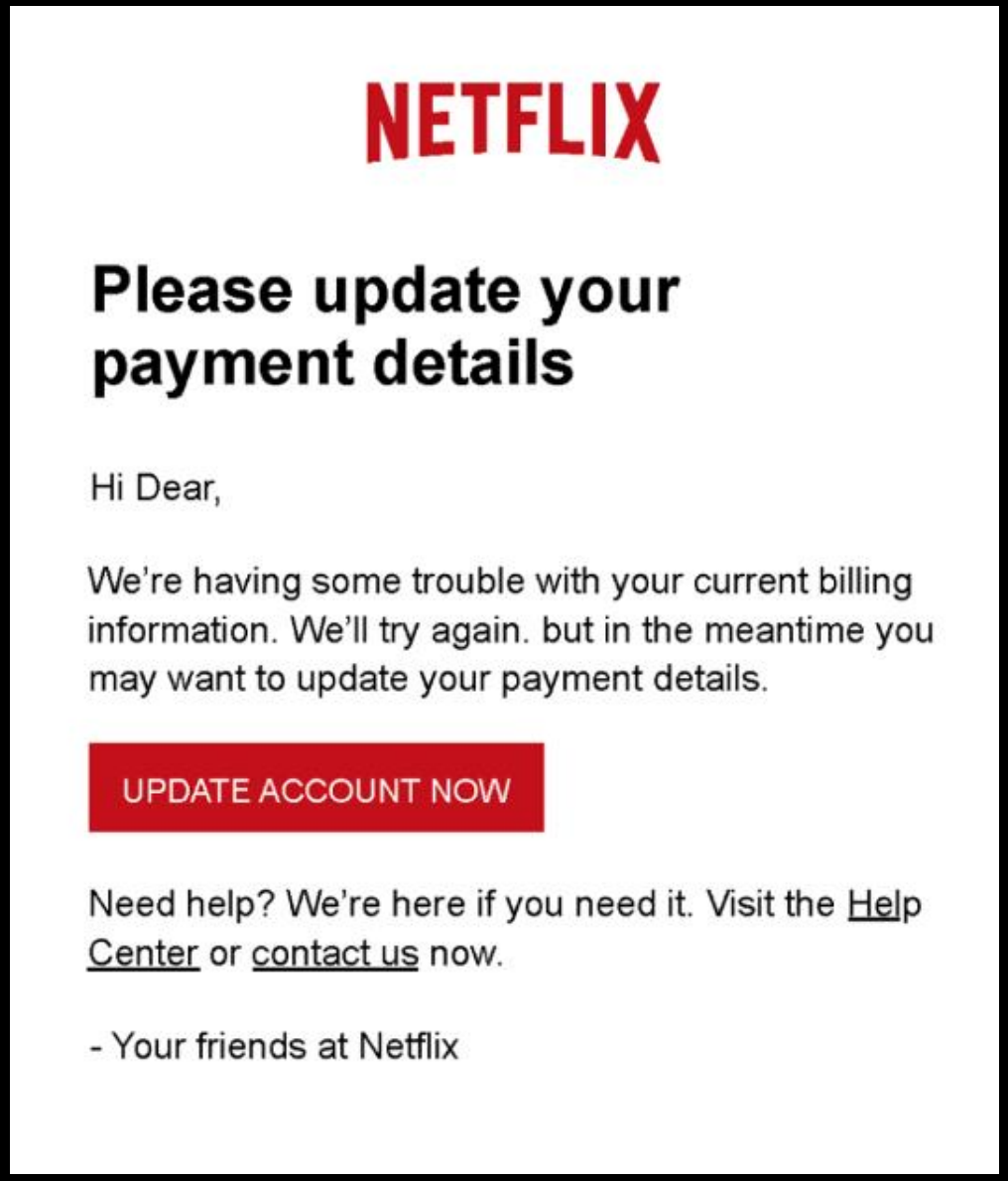
As many of our customers will be aware, Finastra was recently targeted in a cyberattack. As a result of this, on 20th March, we took certain proactive steps to protect our systems and our customers' data, which meant that we had to interrupt service to some customers. First and foremost, we would like to apologize to all affected customers for the inconvenience and concern that this delinquent attack has caused to them and, in turn, their own customers.

In recent weeks the world has seen the number and intensity of cyberattacks increase significantly across all sectors of industry, sadly including even the medical and not-for-profit sectors. These attacks have been deliberately timed to capitalize on the challenges we all face in protecting our colleagues and loved ones from COVID-19. Unfortunately, cyberattacks remain a constant threat for everyone, and we all need to continue to guard against this.

driven

# Phishing Attacks and Business Emails Compromise

Credit unions are often targeted by phishing and BEC attacks, where cybercriminals impersonate employees or executives to trick employees into making fraudulent transactions. These attacks can result in significant financial losses.



NETFLIX

**Please update your payment details**

Hi Dear,

We're having some trouble with your current billing information. We'll try again. but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Need help? We're here if you need it. Visit the Help Center or contact us now.

- Your friends at Netflix

# THINK YOUR BUSINESS IS TOO SMALL TO BE TARGETED BY CYBER CRIMINALS?

An average employee of a small business with less than 100 employees will receive **350%** more social engineering attacks than an employee of a larger enterprise

driven

# Why Cyber Threats Target Small Business?

- No IT Department
- Less likely to follow Internet Best Practices
- Simple network & systems
- Using the cloud
- Using third-party software
- Big Data
- Easy Target

# How We Help Finance Organizations?

# Password and Access Management

- User Account Management
- Role-Based Access Control
- Least Privilege Principle
- Session Management

**Password Practices**

- Complexity
- Length
- Expiration
- Storage
- Recovery

Organizations should continually assess and improve their password and access control policies to adapt to evolving security threats and compliance requirements.


# Employee Training and Awareness Program

Implementing a robust employee training and awareness program is critical for credit unions to enhance cybersecurity, data protection, and overall risk management.

- Social Engineering
- Removable Media
- Mobile Device Security
- Phishing Attacks
- Social Media
- Passwords and Authentication

# Network Defense

Protecting the network infrastructure is essential to ensure the confidentiality, integrity, and availability of member data and financial services.

Firewall

Patch Management

Secure Remote Access

Antivirus

Secure Wi-Fi Networks

# Incident Response and Disaster Recovery

It involves planning, preparation, and response to security incidents to minimize their impact on operations and member data.

Incident Response Plan

Incident Response Team

Incident Identification and Detection

Incident Reporting

TEST, TEST and TEST AGAIN…

# Business Case & Budget Allocation

- Describe the **current cybersecurity posture** of your organization. Include recent security incidents, vulnerabilities, and compliance gaps.
- Clearly **identify the critical assets, data, and systems** that need protection.
- Conduct a comprehensive risk assessment that **quantifies the potential financial, operational, and reputational risks** associated with the current cybersecurity posture.
- Provide a **detailed cost-benefit analysis** that compares the cost of the proposed cybersecurity investments to the potential savings from reduced risks and improved security.


Cybersecurity isn't just an IT problem; it's everyone's responsibility.

# CONTACT US

D-Talks by Driven Advisors

787-725-1500

www.drivenadvisors.com

B7 Tabonuco Street Suite
302 Guaynabo, PR 00968

**Harry Santiago-Perez, CPA, CIA**
hsantiago@drivenadvisors.com
(787) 392-9392

**Josue Hill Felix**
jhill@drivenadvisors.com
(787) 404-7363

**Wilfredo R Vera Pujols, CISA, CDPSE, MCS**
wvera@drivenadvisors.com
(787) 313-7752