RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **AFD-T10**

How to Deploy Secure Technologies to Help Reduce E-Commerce Fraud

Bill Newhouse

Senior Cybersecurity Engineer
National Institute of Standards and Technology
National Cybersecurity Center of Excellence
@cybernewhouse

Learning Objectives

- Frame cybersecurity risks in retail and hospitality sectors
- Learn how to leverage NIST's Cybersecurity Framework to mitigate online fraud
- Explore what technologies can improve cybersecurity and reduce online fraud

RSAConference2020

The Online Retail/Hospitality Landscape & Threats to E-Commerce

Retail & Hospitality Landscape

- Online sales rapidly accelerating, while in-store sales slow
  - Black Friday/Cyber Monday online sales up 20% from previous year
  - In store purchases fell 3% during same period
    (source: Reuters)
- Mobile purchases also rapidly accelerating
  - Mobiles sales will account for $45% of e-commerce by 2020
    (https://www.businessinsider.com/mobile-commerce-shopping-trends-stats)
- Hospitality organizations (hotels) are rapidly embracing IoT and other connected technologies to improve guest experiences.

BRIEF

Retail cyberattack attempts up 20% last year

VIDEOS 5G GUIDE WINDOWS 10 CLOUD AI SECURITY TR PREMIUM MORE NEWSLETTE

AI SECURITY TR PREMIUM MORE NEWSLETTERS

ng

viders were

used to push ransomwa

Once hackers compromise an MSP's network, they can use its

Exposed database left terabyte of

s' data open to the public

Consumer Concern About Holiday Fraud Comes True

iovation research finds 60% rise in suspected holiday weekend e-commerce fraud since 2017, reinforcing consumer worries in recent TransUnion survey

aud Has Tripled. Don't Let It

u

Hotel front desks are now a hotbed for hackers

The hospitality industry can't catch a break when it comes to cybercrime.

s Reporting Data Breaches In

f 2019

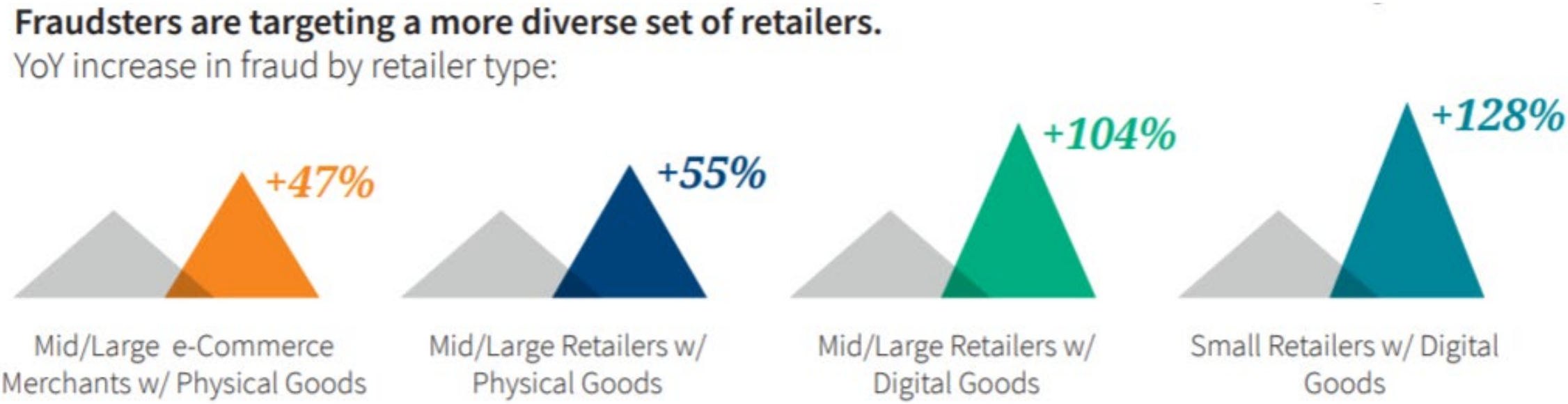
s Safe From Exposed Data Records

E-Commerce Under Threat

- Malicious actors shift from using stolen credit card data in stores at the checkout counter to using stolen credit card data for fraudulent online shopping.

E-Commerce Under Threat

- Retail fraud attempts have TRIPLED since 2017 and each $1 of fraud costs a retailer $3.13.



Source: LexisNexis® Risk Solutions 2019 True Cost of Fraud SM Study - Retail Edition
Available: https://risk.lexisnexis.com/insights-resources/research/2019-true-cost-of-fraud-study-e-commerce-retail-edition

E-Commerce Fraud Scenarios

- Data Breaches – when sensitive data is leaked from a secure location to an untrusted environment
- Phishing or spoofing – when a scammer uses fake email, text messages, or copycat websites to steal your identity or personal information
- Credit card fraud – when scammers obtain money or property through the unauthorized use of a credit or debit card or card number


NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

RSAConference2020

NIST Special Publication 1800-17

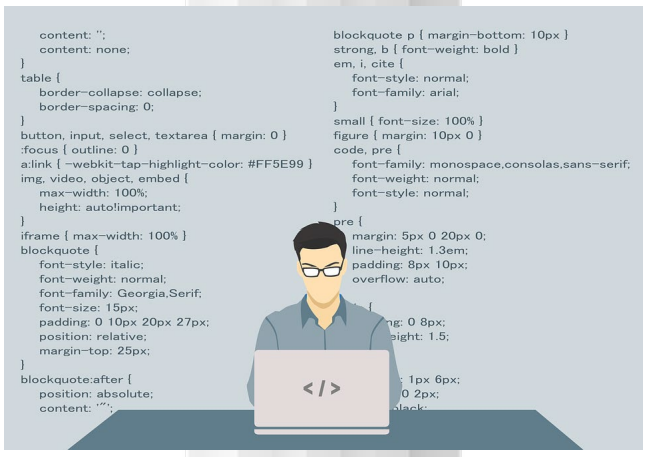
Multifactor Authentication for E-Commerce

Deploying risk-based, Fast Identity Online (FIDO) multifactor authentication to protect online purchases

Protecting the E-Commerce Ecosystem

Customer

Online Shopping Platform



Retail Back Office

Project Capability Goals

- Integrate MFA into online shopping systems
- Mitigate potential exposure to online fraud
- Integrate into a variety of retail-information technology architectures
- Provide authentication options to retailers:
  - Capabilities that assess and mitigate a retailer's shopping transaction risk factors
  - Alert retailer staff to potential threats, and adjust authentication mechanisms as needed

NIST SPECIAL PUBLICATION 1800-17

Multifactor Authentication for E-Commerce

Risk-Based, FIDO Universal Second Factor Implementations for Purchasers

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

William Newhouse
Brian Johnson
Sarah Kinling
Jason Kuruvilla
Blaine Mulugeta
Kenneth Sandlin

This publication is available free of charge from https://doi.org/10.6028/NIST.SP.1800-17

The first draft of this publication is available free of charge from https://www.nccoe.nist.gov/sites/default/files/library/sp1800/cr-mfa-nist-sp1800-17.pdf

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

E-Commerce Fraud Vulnerabilities

E-Commerce organizations can be susceptible to the following vulnerabilities if they possess the certain characteristics.

- Credential stuffing:
  - allow multiple incorrect logins without account lockouts
  - purchasers have reused the same password on multiple systems
- Account takeover:
  - accept weak passwords
  - allow multiple incorrect logins without account lockouts
  - account password-reset options are easily circumvented

Moving Beyond Passwords

"Since most users choose short passwords to facilitate memorization and ease of entry, passwords typically have fewer characters than cryptographic keys. Furthermore, whereas systems choose keys at random, users attempting to choose memorable passwords will often select from a very small subset of the possible passwords of a given length, and many will choose very similar values.

As such, whereas cryptographic keys are typically long enough to make network-based guessing attacks untenable, **user-chosen passwords may be vulnerable, especially if no defenses are in place**."

– NIST Special Publication 800-63-3, *Digital Identity Guidelines*

Standards

- NIST Cybersecurity Framework
- Fast Identity Online (FIDO)

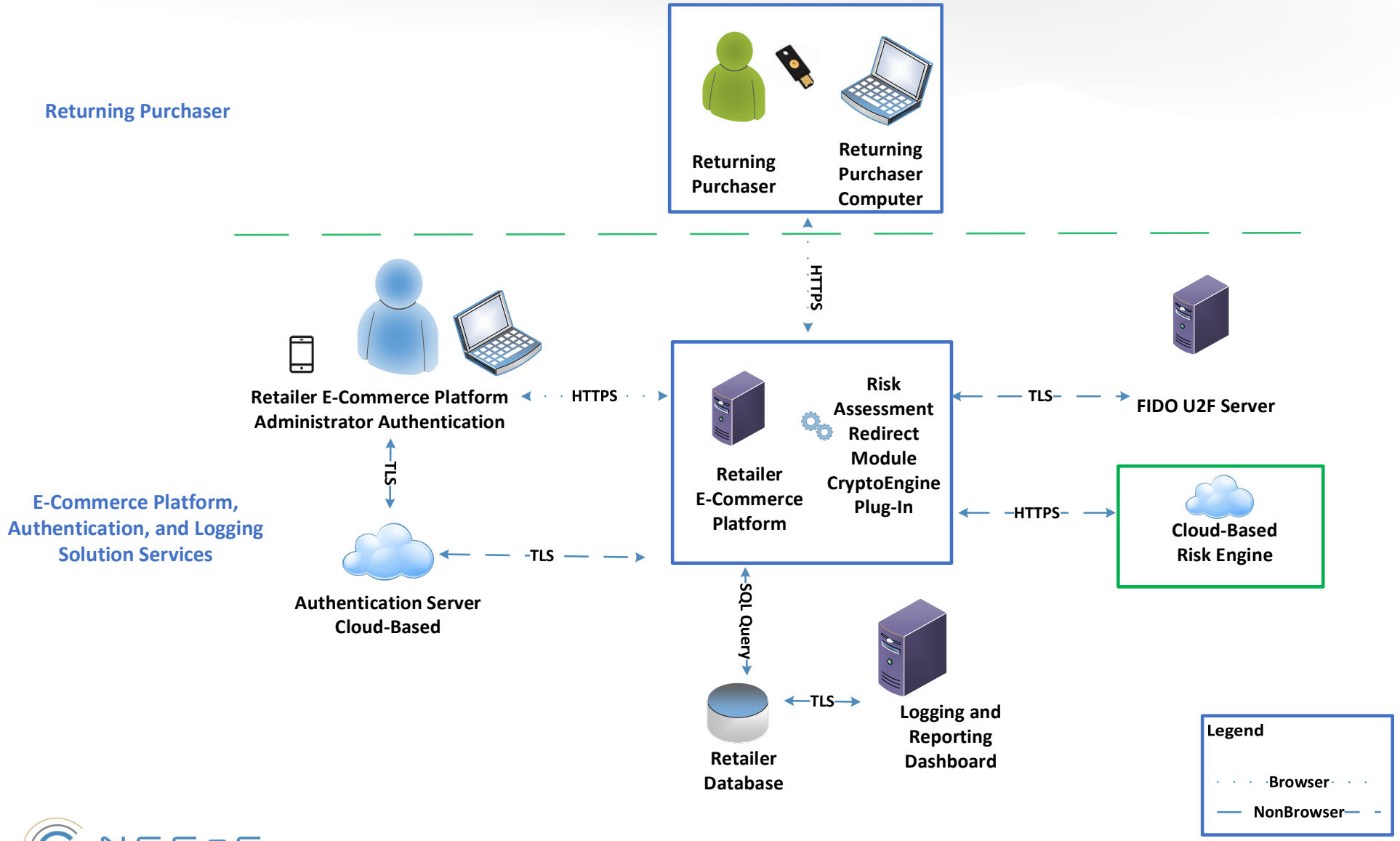
SP 1800-17 Products and Technology

Component	Specific Product	Cybersecurity Framework Subcategories
Retailer E-Commerce Platform	Magento Open Source version 2.1.8	• PR.AC-1 • PR.AC-7 • RS.AN-1
U2F/Risk Assessment Module	Magfido risk assessment policy rules and process module	• ID.RA-4 • ID.RA-5
Risk Engine	RSA Adaptive Authentication (Cloud) 13.1	• ID.RA-4 • ID.RA-5
Multifactor Authentication Mechanism	StrongKey SKCE version 2.0 open-source FIDO U2F Server and TokenOne cloud-based authentication	• PR.AC-1 • PR.AC-7
Multifactor Authenticator	Yubico YubiKey NEO Security Key USB-A ports & Near-field communication (NFC) active devices; TokenOne smartphone application authenticator	• PR.AC-1 • PR.AC-7
Logging / Reporting Dashboard	Splunk Enterprise version 6.6.1	• DE.CM-1

Mapping to Standards (example from NIST SP 1800-17)

Cybersecurity Framework v1.1			Standards and Best Practices Alignment		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Rev 4 Security and Privacy Controls**	**ISO/IEC 27001:2013**	**NIST SP 800-181 NICE Framework Work Role**
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AC)	ID.RA-4: Potential business impacts and likelihoods are identified ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	AC-1 and AC-2: Access Control Family IA-1 - IA-11: Identification and Authentication Family	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3	OM-ANA-001: Systems Security Analyst PR-CDA-001: Cyber Defense Analyst OM-ADM-001: System Administrator OV-PMA-003: Product Support Manager SP-DEV-001: Software Developer

SP 1800-17 Reference Architecture



Benefits of Implementing NIST SP 1800-17

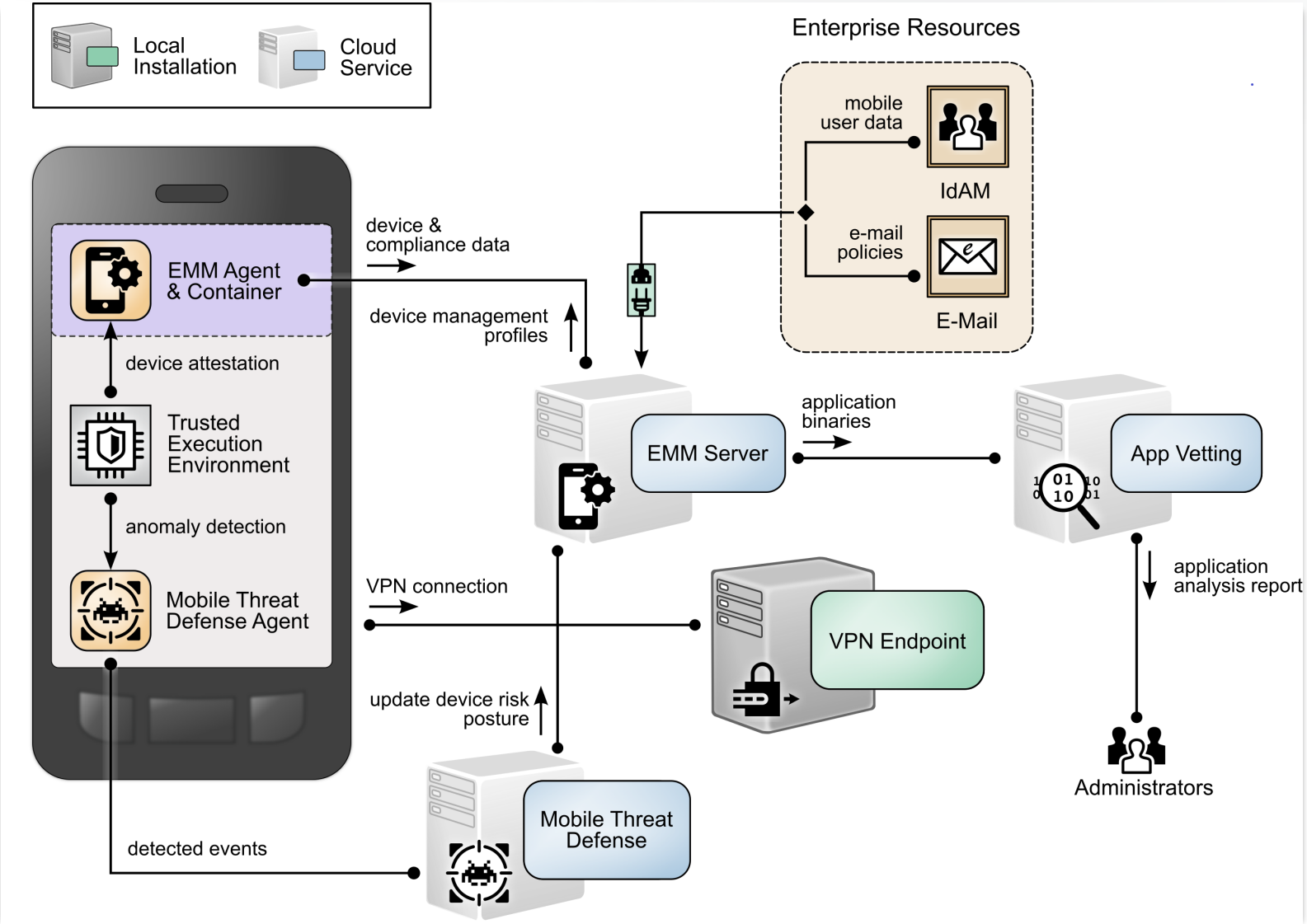
The NCCoE's practice guide to *Multifactor Authentication for E-Commerce* can help your organization:

- reduce online fraudulent purchases
- show customers that the organization is committed to its security
- protect your e-commerce systems
  - *provide greater situational awareness*
  - *avoid system-administrator-account takeover through phishing*
- implement the example solutions by using our step-by-step guide

NCCoE Portfolio

- Attribute Based Access Control (SP 1800-3)
- Consumer/Retail: Multifactor Authentication for e-Commerce (SP 1800-17)
- Data Integrity: Identifying and Protecting
- Data Integrity: Detecting and Responding
- Data Integrity: Recovering (SP 1800-11)
- Derived PIV Credentials (SP 1800-12)
- DNS-Based Email Security (SP 1800-6)
- Energy: Identity and Access Management (SP 1800-2)
- Energy: Situational Awareness (SP 1800-7)
- Financial Services: Access Rights Management (SP 1800-9)
- Financial Services: IT Asset Management (SP 1800-5)
- Healthcare: Securing Electronic Health Records on Mobile Devices (SP 1800-1)
- Healthcare: Securing Wireless Infusion Pumps (SP 1800-8)
- Healthcare: Securing Picture Archiving and Communication Systems (PACS) (SP 1800-24)
- Healthcare: Securing Telehealth Remote Patient Monitoring Ecosystem
- Hospitality: Securing Property Management Systems (SP 1800-27)
- Manufacturing: Capabilities Assessment for Securing Manufacturing Industrial Control Systems
- Mobile Device Security: Cloud and Hybrid Builds (SP 1800-4)
- Mobile Device Security: Enterprise Builds (SP 1800-21)
- Mobile Threat Catalogue
- Privacy-Enhanced Identity Federation
- Public Safety/First Responder: Mobile Application SSO
- Secure Inter-Domain Routing
- TLS Server Certificate Mgmt
- Transportation: Maritime: Oil & Natural Gas
- Trusted Geolocation in the Cloud (NISTIR 7904)

Detailed Reference Architectures Available



RSAConference2020

U.S. Department of Commerce

National Institute of Standards and Technology (NIST)

Information Technology Laboratory

Applied Cybersecurity Division

National Cybersecurity Center of Excellence (NCCoE)

Cybersecurity Framework

Trusted Identities

National Initiative for Cybersecurity Education (NICE)

Privacy Framework

Cybersecurity Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risks.

https://www.nist.gov/cyberframework

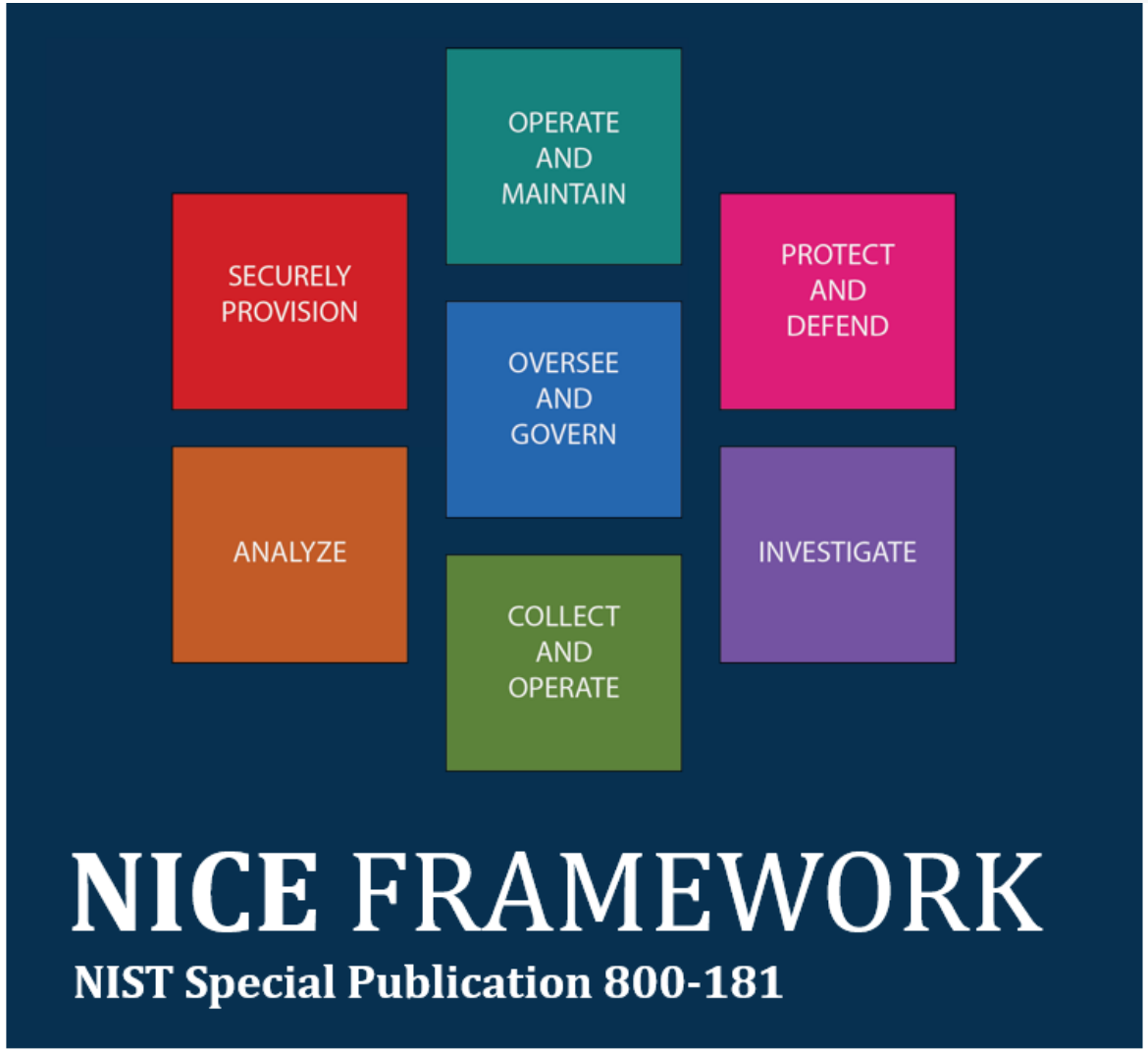
What?

How?

NICE Framework - a taxonomy and common lexicon that describes cybersecurity work and workers

Who?

Workforce Needs to Implement SP 1800-17



1. Improves communication about how to identify, recruit, develop, and retain cybersecurity talent.

2. Categorizes, organizes, and describes cybersecurity work.

3. Can be used by educators, students, employers, employees, training providers, policy makers, and more.

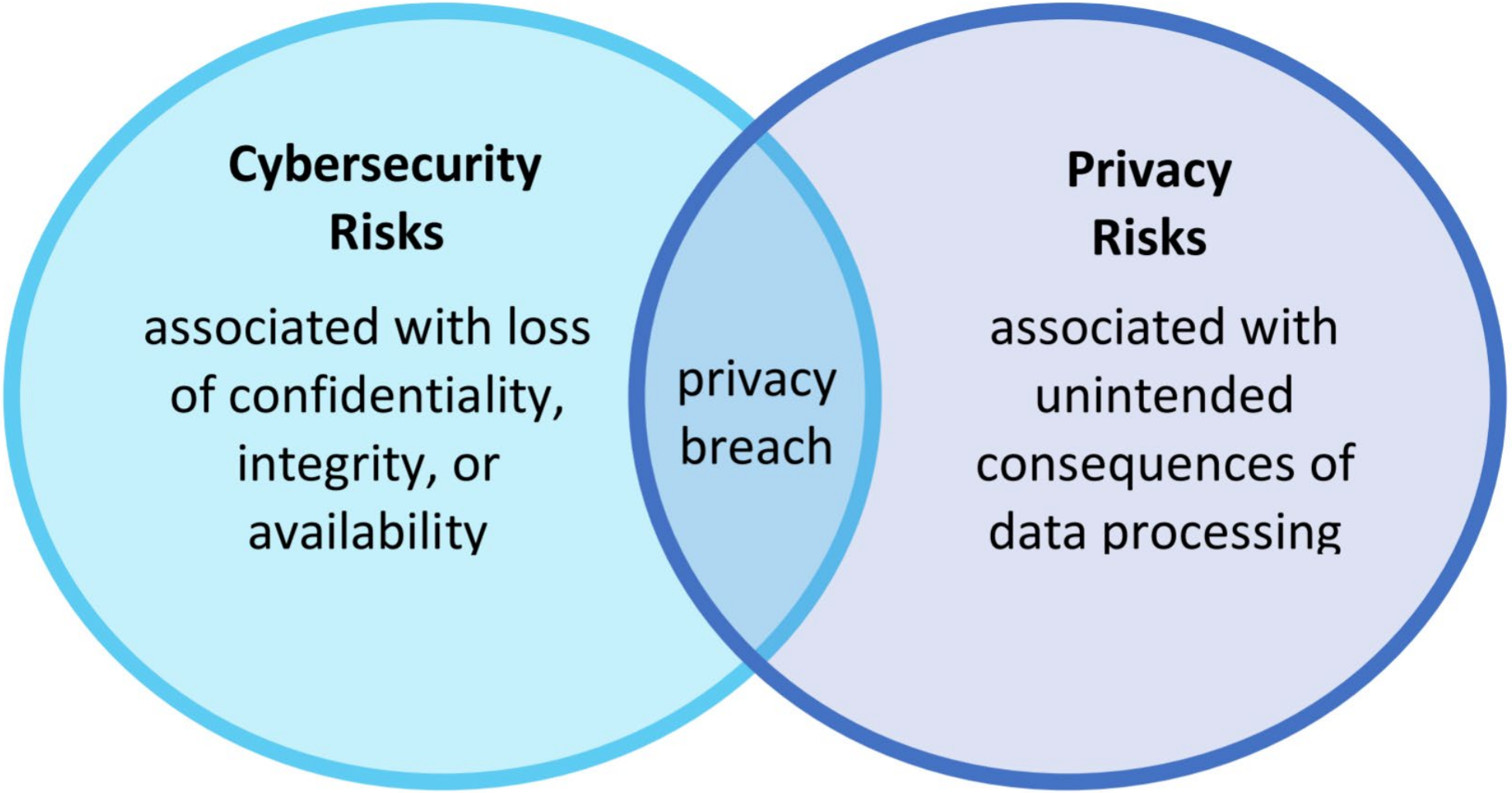
4. nist.gov/nice/framework

RSAConference2020

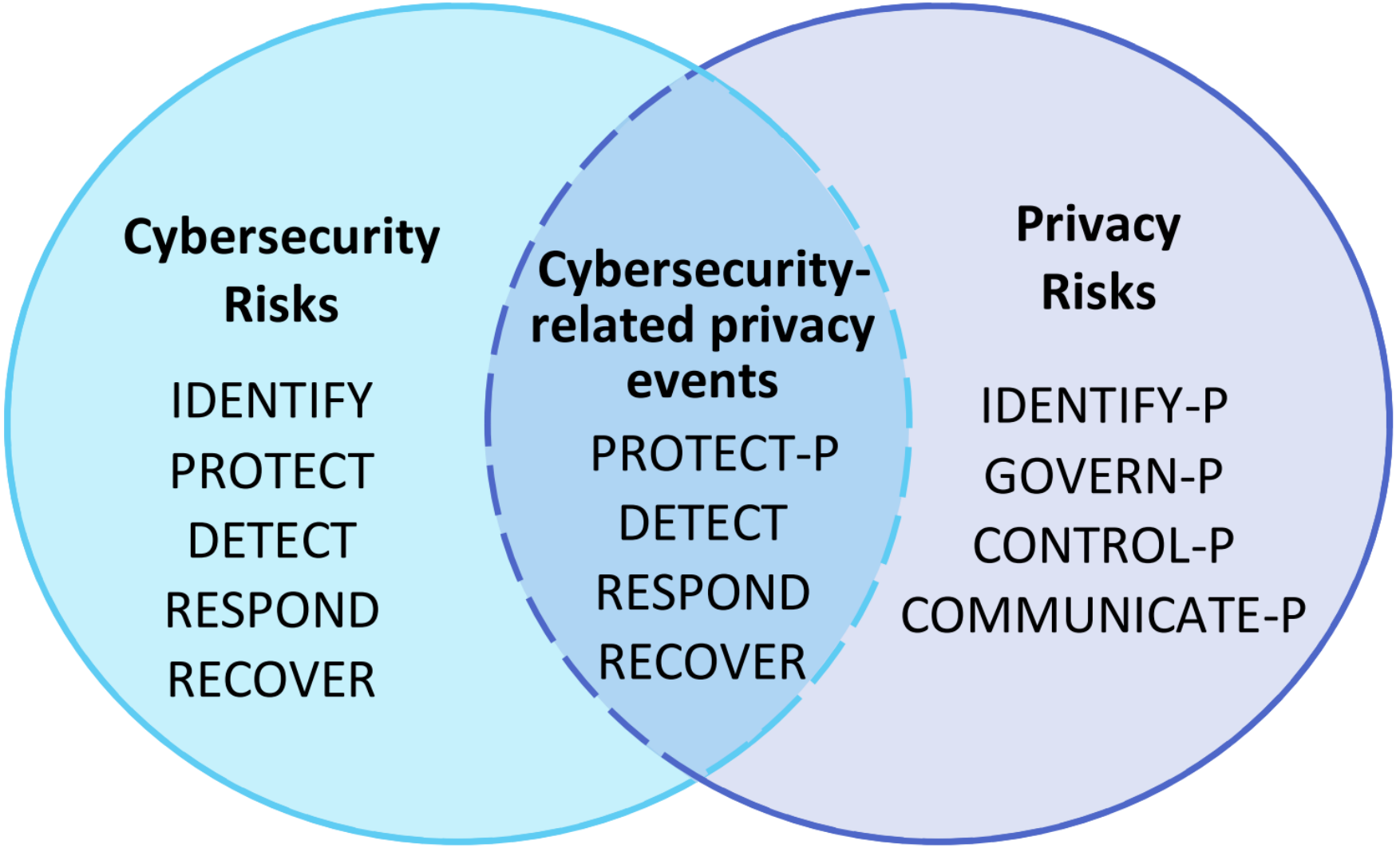
Security and Privacy

Are you addressing privacy risks and the growth in regulations regarding privacy?

NIST Privacy Framework



NIST Privacy Framework



Summary

- Frame cybersecurity risks in retail and hospitality sectors
- Learn how to leverage NIST's Cybersecurity Framework to mitigate online fraud
- Explore what technologies can improve cybersecurity and reduce online fraud

RSAConference2020

Questions?