Panel #1: Identification and Classification of Cyber Risk

- **Steve Bishop**, Head of Risk Information & Insurance, ORX
- **Deborah Bodeau**, Senior Principal Security Engineer, Cyber Solutions Division, The MITRE Corporation
- **Todd Waszkelewicz**, Assistant Vice President, Cybersecurity Policy, Federal Reserve Bank of New York
- **Trevor Watkins**, Risk & Control Manager, PNC
- **Albert Olagbemiro**, Advanced Bank Examiner, Cybersecurity Risk Specialist, Federal Reserve Bank of Richmond
Cyber: a risk management perspective

March 2019

Steve Bishop
Head of Risk Information, ORX

Managing risk together
ORX: Introduction

- Largest operational risk association in the financial services sector.
- Driving the development of operational & non-financial risk management and measurement.
- 97 members – majority of world’s largest financial services firms.
- Owned by our members and not for profit.
- Delivering value to the industry through:
  - Risk information – delivering shared learning & peer benchmarking
  - Research & thought leadership – advancing operational risk management and measurement.
  - Practice – driving risk management standards, including setting industry loss data standards for many years.
  - Events – facilitating member interactions across the globe.
Operational Risk Horizon 2019: Top five risks

**Current risks**

1. **Information security (including cyber)**
   - 89% of participants included an information security risk in their top ten

2. **Conduct**
   - Over a quarter of conduct submissions were specifically concerned with retail mis-selling

3. **Fraud**
   - The third highest risk for the last three years

4. **Transaction processing**
   - Jumps from seventh last year

5. **Technology**
   - 79% of technology submissions expect these risks to increase in the next three years

**Emerging risks**

1. **Digital disruption and disintermediation**
   - Remains number one emerging concern from last year

2. **Information security (including cyber)**
   - 95% expect their submitted risks to materialise in the next three years

3. **Geopolitical and macroeconomic**
   - 63% of all firms ranked it in their top ten

4. **Regulatory compliance**
   - 65% of larger firms ranked this in their top ten

5. **Third party**
   - This risk’s move into the top five is driven by the rise of cloud services

**Top regional risks**

- **Europe**
  - Current: Information security (including cyber)
  - Emerging: Information security (including cyber)

- **Africa**
  - Current: Information security (including cyber)
  - Emerging: Digital disruption and disintermediation

- **North America**
  - Current: Information security (including cyber)
  - Emerging: Information security (including cyber)

- **Asia/Pacific**
  - Current: Information security (including cyber)
  - Emerging: Digital disruption and disintermediation

1. 2. 3. 4. 5.

managingrisktogether.orx.org
British Airways suffers data breach compromising information on 429,000 customer cards

SEC EDGAR database hackers stole files and earned USD 4.1 million through insider trades

Jackson Country pays USD 400,000 ransom to regain control of internal IT systems

Banco de Chile loses USD 10 million and experiences service disruptions during malware attack

Citrix® Hackers access Citrix’s systems using brute force attacks and steal at least 6TB of data
ORX: Cyber risk management challenge

- ORX members report challenges when identifying, categorising and assessing cyber.

  - Basel event types make it difficult to identify and benchmark cyber risk
  - Different perspectives from firms’ Risk and IT teams
  - Financial loss focus a factor in data shortage for assessing risk exposure
  - Difficult to see whether correct controls in place and actions taken
  - The risk has evolved rapidly and doesn’t fit with traditional risk management practices & processes
ORX: Categorising cyber risk

- Members are moving away from the traditional Basel event type categorisation.
- ORX research shows many are developing risk-based taxonomies, supporting risk management activity.
- A proportion include Cyber risk as a unique category. Some instead capture cyber as a flag or theme (‘transversal’ risk), others don’t capture it.
- This inconsistency helps explain the challenge in identifying, classifying and benchmarking the risk within, as well as between firms.

<table>
<thead>
<tr>
<th>Use ‘Cyber’ in taxonomy?</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>48</td>
</tr>
<tr>
<td>No</td>
<td>43</td>
</tr>
</tbody>
</table>

Source: ORX 2018 Taxonomy Report
From 2016, ORX was involved in a trial to identify, collect and categorise cyber & IT incidents.

Categorisation combined IT (based on VERIS and STIX) and operational risk components.

Principles for the trial included:

- Easy to use by different specialists.
- Incidents collected with a range of impacts, including loss, clean up costs, reputational and regulatory.
- Access to data with cooperation between Risk and IT.
- Data collected monthly.
- Allow peer comparison and benchmarking.

An increase in Cyber Risk information began to improve risk management and measurement capability amongst participants.
ORX: Addressing the issue

- Working with members, ORX has now launched O.R.X Cyber to support the active management of cyber risk.

- This is bringing together 2nd Line of Defence cyber risk management specialists, using the ORX ‘Platform’ to:

  ➢ **Share Information** - addressing the risk data shortage and enabling peer benchmarking.

  ➢ **Undertake Research** – looking at risk management and reporting approaches.

  ➢ **Develop Standards** – enhancing practices across the industry.

  ➢ **Improve Collaboration** – through regular, member working groups and forums, as well as with other industry bodies.
ORX: Addressing the issue

Members will benefit through:

➢ Improved data definition, categorisation and identification.

➢ Improved understanding and reporting of cyber risk.

➢ Enhanced cyber risk management practices and peer benchmarking.

➢ Improved understanding between operational risk and cyber risk management teams.

Collaboration among many stakeholders on cybersecurity is critical to progress.

R. Quarles, Vice Chairman for Supervision, The Fed

ORX Cyber will drive improvements in the understanding of risk experience and exposure, enhancing cyber risk management in the industry.
Steve Bishop

Head of Risk Information, ORX

Steve.bishop@orx.org

Follow ORX on LinkedIn

Visit www.orx.org
Panel #1: Identification and Classification of Cyber Risk

- **Steve Bishop**, Head of Risk Information & Insurance, ORX
- **Deborah Bodeau**, Senior Principal Security Engineer, Cyber Solutions Division, The MITRE Corporation
- **Todd Waszkelewicz**, Assistant Vice President, Cybersecurity Policy, Federal Reserve Bank of New York
- **Trevor Watkins**, Risk & Control Manager, PNC
- **Albert Olagbemiro**, Advanced Bank Examiner, Cybersecurity Risk Specialist, Federal Reserve Bank of Richmond
Cyber Threat Modeling in the Identification and Classification of Cyber Risks and Analysis of Cyber Resiliency

Deborah J. Bodeau
Senior Principal Security Engineer
The MITRE Corporation
dbodeau@mitre.org
Cyber Risk and Cyber Resiliency Can Be Considered at a Range of Scopes or Scales

- Sector or Region
- Sub-Sector / Multi-Organization Function System-of-Systems
- Organization
- Mission / Business Function System-of-Systems
- Technical System (ICT, CPS)
Cyber Risk and Cyber Resiliency Are Closely Related

**Cyber Risk**

- The *risk of depending on cyber resources*, i.e., the risk of depending on systems or system elements which exist in or intermittently have a presence in cyberspace.
- Consider (may focus on) adversarial threat actors operating in cyberspace.
- Often evaluated as *likelihood* for a defined impact or set of consequences (e.g., data breach).

**Cyber Resiliency**

- The ability to *anticipate, withstand, recover from, and adapt to adverse conditions*, stresses, attacks, or compromises on systems that use or are enabled by *cyber resources*.
- Focus on advanced cyber adversaries, who may emulate or leverage threat events from other sources.
- Enables definition and evaluation of strategies, practices, and technologies to reduce *consequence severity* as well as likelihood of subsequent events, assuming the success of prior threat events.
Cyber risk to a system is a function of

- Threats
- The structure, characteristics, and behaviors of the system
  - Characteristics can include vulnerabilities
- The consequences of threats materializing or acting on the system
  - Can be identified with asset loss
- In an (assumed or observed) operational environment

Decrease in cyber risk to a system is one measure of the effectiveness of a cyber resiliency solution
Starting with Threats Can Simplify Discussions and Facilitate Characterization and Identification

▪ Avoid the need to share sensitive information about
  – System structure, behavior, or vulnerabilities
  – Potential or past consequences

▪ Avoid arguments about how best to describe systems and vulnerabilities

▪ But starting with “threat” requires qualification
  – Threat source ≠ threat event ≠ threat scenario
The Cyber Threat Component of Cyber Risk Can Be Used in Multiple Ways

Cyber Threat Model

- Risk Modeling, Analysis, Assessment
  - Assess likelihood of threat scenarios or threat events that produce identified consequences
- Cyber Wargaming
  - Determine operational resilience, cyber resiliency in context of representative threat scenarios, stresses, and operations
- Cyber Threat Coverage Analysis
- Analysis of Alternatives
  - Analyze the potential decrease in risk, ability to achieve cyber resiliency objectives, in the context of assumed threat characteristics
- Threat Intelligence Information Sharing
  - Share information about threat characteristics, observed threat events, observed or posited threat scenarios in the form of cyber campaigns
- Detection and Forensic Analysis
  - Determine characteristics of observed threat events, threat scenarios
Threat Models Can Include Many Factors …

Color Key:
- Threat Source
- Threat Event
- Threat Scenario

Dashes indicate links to risk assessment

Threat Source → Threat Event

Threat Source

Threat Type (adversarial, etc.)

Characteristic (depends on Threat Type)

Threat Scenario

Consequence

Consequence Type

Severity

Stakeholder

Effect Type (cyber, non-cyber)

Effect

Likelihood of Success

Likelihood of Occurrence

Location

Duration

is involved in (causes one or more events in)

is part of (causes one or more events in)

leads to or is part of

has

causes
... Even When Restricted to Adversarial Threats Against Cyber Resources
But Factors Irrelevant to an Intended Use Can Be Disregarded, Enabling Focus to Be Driven by Use

Focus on factors with, or determinant of, Likelihood or Severity (may downplay some adversary characteristics)

Consider Cyber Effects of Threat Events, to look for artifacts and indicators

Consider Cyber Effects of Threat Events, to share information about artifacts and indicators

Consider adversary characteristics related to intent and targeting, to share information about campaigns

Consider factors with, or determinant of, Likelihood or Severity

Define representative Threat Scenarios, considering Threat Events and their characteristics; only consider adversary characteristics to motivate Scenarios

Consider potential effects on and coverage of Threat Events
One Common Theme ... Identify Threat Events Using a Framework Following the Structure of a Threat Scenario or Cyber Campaign

A variety of frameworks are available, including:
- Cyber Kill Chain™ framework
- NIST SP 800-30R1: cyber attack lifecycle (CAL) stages, representative events
- ATT&CK™
- ODNI Cyber Threat Framework
- NSA Technical Cyber Threat Framework V2
A Common Framework for Identifying Threat Events Supports Cyber Threat Coverage Analysis at Different Levels of Description

Example: Potential effects of cyber resiliency techniques and implementation approaches on adversary objectives, using the NSA Technical Cyber Threat Framework

<table>
<thead>
<tr>
<th>Objective</th>
<th>Cyber Resiliency Technique</th>
<th>Implementation Approach</th>
<th>Execution</th>
<th>Internal Reconnaissance</th>
<th>Privilege Escalation</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Persistence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Response</td>
<td>Dynamic Reconfiguration</td>
<td>Negate, Delay, Exert</td>
<td>Exert, Shorten</td>
<td>No effect</td>
<td>No effect</td>
<td>Contain</td>
<td>No effect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamic Resource Allocation</td>
<td>No effect</td>
<td>Delay, Exert, Shorten</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
<td></td>
</tr>
<tr>
<td>Adaptive Management</td>
<td>Delay, Preempt, Shorten, Reduce</td>
<td>No effect</td>
<td>Shorten, Reduce</td>
<td>No effect</td>
<td>No effect</td>
<td>Preempt, Negate</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Objective</th>
<th>Analytic Monitoring</th>
<th>Sensor Fusion &amp; Analysis</th>
<th>Forensic &amp; Behavioral Analysis</th>
<th>Contextual Awareness</th>
<th>Mission Dependency &amp; Status Visualization</th>
<th>Coordinated Protection</th>
<th>Consistency Analysis</th>
<th>Orchestration</th>
<th>Self-Challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring &amp; Damage Assessment</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic Resource Awareness</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic Threat Awareness</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mission Dependency &amp; Status Visualization</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
<td>No effect</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Examples of Research actions:</th>
<th>Examples of Reconnaissance actions:</th>
<th>Examples of Delivery actions:</th>
<th>Examples of Execution actions:</th>
<th>Examples of Monitor actions:</th>
<th>Examples of Evasion actions:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Gather information</td>
<td>Conduct social engineering</td>
<td>Alter communications</td>
<td>Create scheduled</td>
<td>Activate recording</td>
<td>Block indicators or</td>
</tr>
<tr>
<td></td>
<td>Identify capability gaps</td>
<td>Send malicious content</td>
<td>Use legitimate rem</td>
<td>Replace existing</td>
<td>Log keystrokes</td>
<td>Obfuscate data</td>
</tr>
<tr>
<td></td>
<td>Identify Information gaps</td>
<td></td>
<td></td>
<td>Write to disk</td>
<td></td>
<td>Remove toolkit</td>
</tr>
</tbody>
</table>

© 2019 The MITRE Corporation. All rights reserved.
A Common Framework for Identifying Cyber Threat Events Can Align Different Uses and Different Scales ...

Example: Aligning Analysis of Alternatives and Cyber Wargaming within an organization
... As Well as Extension to Systems-of-Systems Beyond a Single Organization

- Identify systemic cyber risks, cyber resiliency gaps, and risk governance issues
- Identify gaps in
  - Widely-deployed / sector-standard technologies and practices
  - Threat and incident information sharing
- Develop cyber wargames to promote cross-organizational efforts

- Identify enterprise cyber risks, cyber resiliency gaps, and risk governance issues
- Identify gaps in
  - Cybersecurity and resilience technologies and practices
  - Cyber playbooks and Security Operations Center capabilities
- Develop cyber wargames involving threats to the enterprise

- Identify gaps in
  - Cybersecurity and resilience technologies and practices
  - COOP and contingency planning
- Develop cyber wargames involving threats to accomplishing the mission or business function

Example of uses of threat scenarios involving systems-of-systems
Conclusion

- Any discussion of risk overlaps with or impinges on discussions of other topics ... particularly resilience

- Analysis of cyber risk — and of cyber resiliency — informs and can be informed by a variety of other activities, including
  - Threat intelligence information sharing
  - Cyber wargaming
  - Analysis of alternatives for strategies, system design, operations

- Use of a common threat modeling framework can bring consistency to these activities, both within an enterprise and beyond
For More Information …


**Publications in this collection include:**
- Cyber Threat Modeling: Survey, Assessment, and Representative Framework
- Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context
- Advanced Cyber Risk Management: Threat Modeling & Cyber Wargaming Briefing
- Enhanced Cyber Threat Model for Financial Services Sector Institutions
- Enterprise Threat Model Technical Report-Cyber Threat Model for a Notional Financial Services Sector Institution
- System-of-Systems Threat Model
- Cyber Risk Metrics Survey, Assessment and Implementation Plan Report
- Cyber Risk Metrics Survey, Assessment and Implementation Plan Briefing
- Financial System Mapping
- Dynamic Data Map Technical Report

MITRE’s mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more [www.mitre.org](http://www.mitre.org)
Panel #1: Identification and Classification of Cyber Risk

- **Steve Bishop**, Head of Risk Information & Insurance, ORX
- **Deborah Bodeau**, Senior Principal Security Engineer, Cyber Solutions Division, The MITRE Corporation
- **Todd Waszkelewicz**, Assistant Vice President, Cybersecurity Policy, Federal Reserve Bank of New York
- **Trevor Watkins**, Risk & Control Manager, PNC
- **Albert Olagbemiro**, Advanced Bank Examiner, Cybersecurity Risk Specialist, Federal Reserve Bank of Richmond
Cyber Risk Workshop: Risk Identification
Federal Reserve Bank of Richmond – Charlotte Branch

Todd Waszkelewicz
Federal Reserve Bank of New York; Supervision Group – Cybersecurity Policy
March 28, 2019
The views that I express are my own and do not necessarily represent those of the Federal Reserve Bank of New York or the Federal Reserve System.
Strengthening Risk Identification

Ongoing priorities

- Enhancing abilities to assess the impact of current and future cybersecurity events in the financial sector
  - Support supervisory staff in identifying, assessing and monitoring cyber risks
  - Support supervisory leaders in making data-driven decisions to better allocate policy priorities, examination focus and resources to the top risks affecting the financial sector
  - Strengthen context and understanding in response to cyber events

Examples of key initiatives to strengthen cyber risk identification

- Scenarios analysis to better contextualize cyber risks
- Mapping of financial sector interconnectedness
Scenario Analysis

- Risk analysis process to identify top risks and develop cybersecurity supervisory themes for the next supervisory cycle

- One component of the process is to conduct scenario analysis to identify and prioritize top risks

- Utilize industry framework to estimate risks (e.g., Factor Analysis of Information Risk (FAIR))

- Enumerate plausible and concerning cybersecurity-related risk scenarios for the U.S. financial sector

- Leverage SMEs to estimate the likelihood and impact for each risk scenario using the FAIR framework

- Associate control categories related to preventing and mitigating the highest ranking scenarios

- Develop supervisory themes that incorporate the related control areas adjusting for other inputs
Why use an Industry framework such as FAIR

Factor Analysis of Information Risk (FAIR)

• Helps achieve a central objective of identifying, evaluating and comparing cybersecurity risk events
• Provides a common framework and language for SMEs to use in estimates
• No need for additional tools/software to use the methodology
• Gaining traction in industry
Financial Services Sector is highly interconnected and interdependent which increases its attack surface and the proliferation of cyber risks.

Risk to critical functions and systems continue to build as sophistication and focus of threat actors increases.

Establishing a data-driven analytical capability to map interconnectedness and assess impact of cybersecurity risks in the financial sector.

- Map and visualize the interconnectedness of critical financial markets
- Enhance analytical capabilities to identify and assess vulnerabilities and implications
- Strengthen context and understanding in response to cyber events

We are aiming to answer questions such as:
- What is the potential impact of a particular cyber event or scenario on a firm or critical financial market?
- What are the interdependencies or concentrations that could pose risk?
- What are the areas of greatest concern?
Analyzing the breadth, depth and complexity of Interconnectedness

Identifying key players

Identifying key financial market utilities and agents supporting a key player
Identifying key dependencies

- Key agent dependency across two top players in a critical financial market
Identifying patterns in risk

- Relate supervisory issues to common industry frameworks (e.g., NIST Cybersecurity Framework (CSF))
- Data for three top players show an overlap in supervisory criticisms related to information protection; in particular, vulnerability management
- Collectively, these firm accounted for xx% of value of a critical financial market

Weaknesses identified in the development and/or implementation of a vulnerability management plan
Summary

- Interconnectedness mapping and analysis enables us to bring together disparate data sources (e.g., organizational, supervisory and transactional data) into one analytic platform to identify concentrations of risk and potential impact of cyber risks.

- Scenario analysis helps us to drive supervisory focus to top risks in the financial sector.
Panel #1: Identification and Classification of Cyber Risk

- **Steve Bishop**, Head of Risk Information & Insurance, ORX
- **Deborah Bodeau**, Senior Principal Security Engineer, Cyber Solutions Division, The MITRE Corporation
- **Todd Waszkelewicz**, Assistant Vice President, Cybersecurity Policy, Federal Reserve Bank of New York
- **Trevor Watkins**, Risk & Control Manager, PNC
- **Albert Olagbemiro**, Advanced Bank Examiner, Cybersecurity Risk Specialist, Federal Reserve Bank of Richmond
Cyber Risk Workshop
Identification and Classification
Who We Are

- **Overview and Background**
  - PNC is one of the largest diversified financial services institutions in the United States
  - Employees in more than 40 states across the country
  - Regional presidents in 39 market
  - A retail branch network stretching across 19 states and the District of Columbia
  - Strategic international offices in Canada, China, Germany and the U.K.
PNC’s definition of Operational Risk closely aligns to the BASEL definition and defines risk arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events.

PNC follows an Operational Risk Framework that layers into an Enterprise Risk Management Framework ensuring the management of risk is consistent across PNC.

PNC has classified all risks into risk categories known as risk taxonomy.

Figure 1: Risk Taxonomies
## PNC Operational Risk Domains

<table>
<thead>
<tr>
<th>Icon</th>
<th>Domain</th>
<th>Focused on managing:</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Operations" /></td>
<td><strong>Operations (People/Processes)</strong></td>
<td>Risk resulting from inadequate or failed internal processes, misconduct or errors of people and fraud</td>
</tr>
<tr>
<td><img src="image" alt="Compliance" /></td>
<td><strong>Compliance</strong></td>
<td>Risk associated with failure to comply with applicable laws and regulations or contractual obligations</td>
</tr>
<tr>
<td><img src="image" alt="Data Management" /></td>
<td><strong>Data Management</strong></td>
<td>Risk associated with incomplete or inaccurate data</td>
</tr>
<tr>
<td><img src="image" alt="Model" /></td>
<td><strong>Model</strong></td>
<td>Risk associated with the design, implementation, and ongoing use and management of a model</td>
</tr>
<tr>
<td><img src="image" alt="Technology &amp; Systems" /></td>
<td><strong>Technology &amp; Systems</strong></td>
<td>Risk associated with use, operation and adoption of technology</td>
</tr>
<tr>
<td><img src="image" alt="Information Security" /></td>
<td><strong>Information Security</strong></td>
<td>Risk resulting from the failure to protect information and ensure appropriate access to, and use and handling of information assets</td>
</tr>
<tr>
<td><img src="image" alt="Business Continuity" /></td>
<td><strong>Business Continuity</strong></td>
<td>Risk of potential disruptive events to business activities</td>
</tr>
<tr>
<td><img src="image" alt="Third Party" /></td>
<td><strong>Third Party</strong></td>
<td>Risk arising from failure of third party providers to conduct activity in a safe and sound manner and in compliance with contract provisions, applicable laws and regulations</td>
</tr>
</tbody>
</table>
Identification and Classification of Cyber Risk

**Identification through Trigger Events**

- **External Loss Data (ELD)**
  - The review of loss events experienced by other institutions for applicability to PNC
  - Analysis of root cause and trends
  - Proactive approach to risk and control enhancement through a systematic process

- **Internal Loss Data (ILD)**
  - Expenses associated with an operational loss event
  - Capture and analyze ILD root causes and trends to improve ORM capabilities

- **Issues**
  - Failure of a control or lack of a control
  - Determine corrective action or resolution
  - Lifecycle
    - Identification and Investigation
    - Action Planning and Management Response
    - Monitoring and Reporting
    - Resolution

**Classification**

- Trigger Identification Source
- Assigned Risk Domain
  - Risk Categories (aka Risk Taxonomies)
- Process Detailed Risks (Level 3)
  - Process Categories (Level 1)
  - Process Significant Risks (Level 2)
BankIslami loses PKR 2.6 million after cyberattack on payment card network.

On 29 October 2018, it was reported that PKR 2.6 million (USD 19,000, EUR 17,000) had been stolen from BankIslami customer accounts after hackers compromised the bank’s international payment card network and conducted debit card transactions.

According to BankIslami, the cyberattack was a coordinated attack against the payment network of its international payment scheme and the payment networks of the acquiring banks, the News International reports. One source told Profit that “there is a clear breach of information at BankIslami’s part” and a digital copy of BankIslami customers’ credit card information may have been leaked to hackers.

The bank has informed Pakistan’s central bank of the attack, which instructed BankIslami to advise customers on precautionary measures to take, and engaged information security experts. BankIslami restored all domestic ATM cash withdrawals using biometric services on 27 October 2018, but as of 28 October 2018 was yet to restore transactions routing through its international payment scheme.
Over 77 million T-Mobile customer account PINs exposed due to Apple website security flaw

On 24 August 2018, Buzzfeed News reported that a security flaw in Apple’s online store had inadvertently exposed over 77 million T-Mobile customer account PINs, which often constitute the last four digits of a customer’s Social Security Number (SSN).

When purchasing an iPhone through Apple’s online store, customers are prompted to select a carrier and monthly payment plan. If T-Mobile is selected, customers are redirected to an authentication page which asks for their T-Mobile phone number and account PIN or the last four digits of their SSN.

The T-Mobile authentication page did not limit the number of entry attempts. This meant that hackers could use widely-available hacking software to repeatedly enter random combinations of numbers to guess the customer’s PIN, a method known as a brute-force attack.

Ceraolo stated that the vulnerability was most likely caused by an engineering mistake made when connecting T-Mobile’s account validation application programming interface (API) to Apple’s website. The API allows Apple access to T-Mobile’s customer data in order to validate customer logins. If a hacker obtains an account PIN in combination with the correct phone number, they would then be able to pose as the genuine customer to “hijack” the SIM card by contacting the carrier and requesting that calls and texts are transferred to another phone number.
Commonwealth Bank of Australia (CBA) has been unable to locate two magnetic data tapes containing the records of 19.8 million customers after a subcontractor failed to provide documentation that it had destroyed them.

Buzzfeed names the subcontractor as Fuji Xerox, which in 2016 decommissioned the data centre where CBA customer data was stored. The tapes were due to be destroyed, but on 9 May 2016 the bank had not received documentation to confirm this had taken place.

Subsequently, on 20 May 2016, CBA informed the Office of the Australian Information Commissioner (OAIC) and the Australian Prudential Regulation Authority (APRA) that it was unable to locate the tapes. The magnetic data tapes were used to print bank statements and contained names, addresses, account numbers and transaction details from between 2000 and 2016. According to CBA, the tapes did not contain passwords, personal identification numbers (PIN) or other data that could enable fraud.
Discussion & Questions