RSAConference2018

Singapore | 25–27 July | Marina Bay Sands

#RSAC

SESSION ID: SDS-R08

# APPROPRIATE INFORMATION SECURITY RISK MANAGEMENT FOR TODAY AND THE FUTURE

**Peter Van Loon**

Senior Manager, Information Security Risk
Discover Financial Services

# Overview

**Information security is a risk management function today and deployed protections must be aligned to risk to maintain an appropriate risk posture**

**Presentation:**

- Practices and considerations common historically and today
- Conclusions and recommendations on practices necessary today and in the future
- Sample cases demonstrating applicability of recommendations

**Agnostic Messages:** Practices reviewed are applicable and may be adapted to all organizations

The opinions expressed in this presentation are those of the presenter, in their individual capacity, and not necessarily those of Discover

# Background

**What is Information Security Risk?**

- NIST 800-30: “Risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization”
- Information security rapidly evolved over the past 30+ years and is now a risk management function
- Focus historically was not placed on dedicated information security risk management, function was practiced informally

**Context today?**

- Varied importance placed on function
- Informal and inconsistent practices are common
- Compliance (e.g. PCI DSS) commonly drives information security risk management activities
- Industry standards provide broad guidance
- Sophisticated risk management practices present in few organizations (e.g. robust KRIs, formal risk committees)

# Information Security Risk

### What are Core Components?[1]

- **Threat Actor:** Human or non-human entity that exploits a vulnerability
- **Vulnerability:** That which the threat actor exploits
- **Outcomes:** The result of exploiting a vulnerability
- **Impact:** Consequences from unwanted outcomes
- **Likelihood:** The likelihood of a scenario is portrayed by a threat exploiting vulnerability with a given probability
- **Information Asset:** Informational element (e.g. data, process) that was affected by the risk

### Risk Treatment:

- Inherent Risk = **Mitigation / Transfer** + Residual Risk
- **Acceptance**
- **Avoidance**

**Key Inherent Challenges:** Measurement and Management

[1] Information Security Risk Management: Understanding the Components; Peter Sullivan, TechTarget

# Core Components - Examples

## Examples of Core Components?

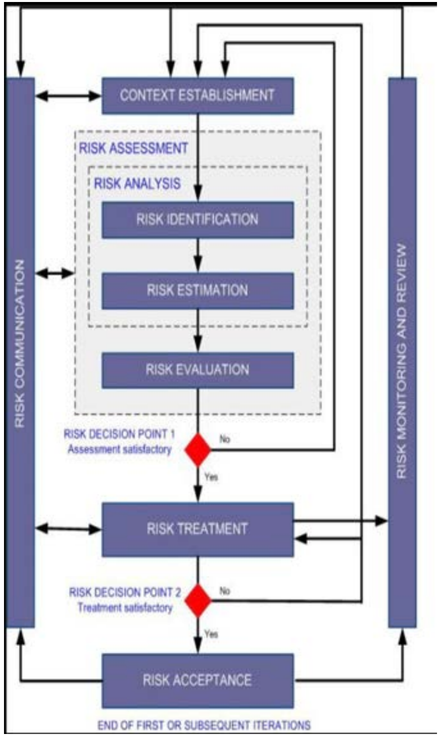
- **Threat Actor:** Hacktivist, cyber-criminal, insider threat
- **Vulnerability:** Misconfigured system, unprotected web application
- **Outcomes:** Acquisition of sensitive data, in-availability of key system or service
- **Impact:** Cost of breach, reputational damage, fines
- **Likelihood:** Once a year, once a minute
- **Information Asset:** Data, informational platform

## Sample Information Security Risk Statement:

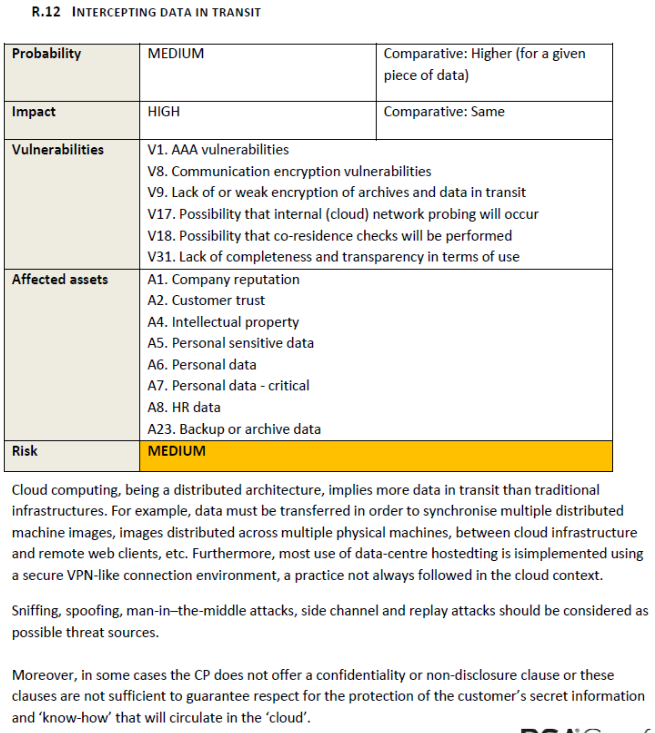
‘A cybercriminal may compromise a web application handling personally identifiable information to obtain a 1,000 records’

# Information Security Risk Assessment

## ISO 27005 Risk Management Framework[2]



## Sample Output – Individual Risk[3]



**R.12 INTERCEPTING DATA IN TRANSIT**

| | | |
|---|---|---|
| **Probability** | MEDIUM | Comparative: Higher (for a given piece of data) |
| **Impact** | HIGH | Comparative: Same |
| **Vulnerabilities** | V1. AAA vulnerabilities<br>V8. Communication encryption vulnerabilities<br>V9. Lack of or weak encryption of archives and data in transit<br>V17. Possibility that internal (cloud) network probing will occur<br>V18. Possibility that co-residence checks will be performed<br>V31. Lack of completeness and transparency in terms of use | |
| **Affected assets** | A1. Company reputation<br>A2. Customer trust<br>A4. Intellectual property<br>A5. Personal sensitive data<br>A6. Personal data<br>A7. Personal data - critical<br>A8. HR data<br>A23. Backup or archive data | |
| **Risk** | **MEDIUM** | |

Cloud computing, being a distributed architecture, implies more data in transit than traditional infrastructures. For example, data must be transferred in order to synchronise multiple distributed machine images, images distributed across multiple physical machines, between cloud infrastructure and remote web clients, etc. Furthermore, most use of data-centre hostedting is isimplemented using a secure VPN-like connection environment, a practice not always followed in the cloud context.

Sniffing, spoofing, man-in–the-middle attacks, side channel and replay attacks should be considered as possible threat sources.

Moreover, in some cases the CP does not offer a confidentiality or non-disclosure clause or these clauses are not sufficient to guarantee respect for the protection of the customer's secret information and 'know-how' that will circulate in the 'cloud'.

[2] Al-Safwani, Nadher & Hassan, Suhaidi & Katuk, Norliza. (2014). A Multiple Attribute Decision Making for Improving Information Security Control Assessment.
[3] ENISA Cloud Computing Risk Assessment, 2009

# Core Challenge - Measurement

**Definition of Measurement:** Expressed reduction of uncertainty based on one or more observations[4]

**Core components such as Threat Actors and Likelihood are especially difficult to quantify and are commonly qualitatively expressed**

**“Uncertainty Reduction” foundation of measurement, basis originates in ‘Information Theory’ [Claude Shannon, 1948]:** Proposal of a mathematical definition of “information” as the amount of uncertainty (“entropy”) reduction removed in a signal

[4] How to Measure Anything in Cybersecurity Risk; Douglas Hubbard and Richard Seiersen

# Core Challenge - Management

At all times, information security risk affecting an organization should be:

- Aligned and supportive to business objectives
- Identified and assessed
- Compared against risk appetite and treated accordingly
- Monitored for changes
- Reported and incorporated into enterprise risk management practices

**Effectiveness of information security programs and investment dependent on appropriate and harmonized risk management functions**

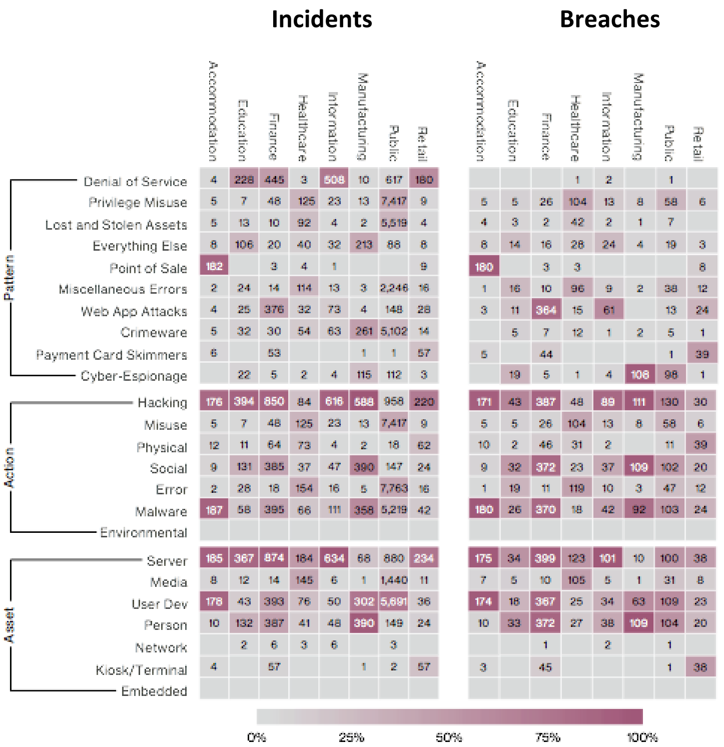
# Industry Variances

## Distinct Incident and Event Differences Exist - Retail Industry Example (2017):

- **Significant Incidents**: 55% were denial of service, 18% were payment card skimming
- **Significant Breaches:** 41% were payment card skimming, 26% were web application attacks

**Influence:** Weight should be applied to core components (e.g. likelihood) ratings based on industry

Verizon DBIR 2017[5]



|  |  | Incidents |  |  |  |  |  |  |  | Breaches |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  | Accommodation | Education | Finance | Healthcare | Information | Manufacturing | Public | Retail | Accommodation | Education | Finance | Healthcare | Information | Manufacturing | Public | Retail |
| Pattern | Denial of Service | 4 | 228 | 445 | 3 | 508 | 10 | 617 | 180 |  |  |  | 1 | 2 |  | 1 |  |
|  | Privilege Misuse | 5 | 7 | 48 | 125 | 23 | 13 | 7,417 | 9 | 5 | 5 | 26 | 104 | 13 | 8 | 58 | 6 |
|  | Lost and Stolen Assets | 5 | 13 | 10 | 92 | 4 | 2 | 5,519 | 4 | 4 | 3 | 2 | 42 | 2 | 1 | 7 |  |
|  | Everything Else | 8 | 106 | 20 | 40 | 32 | 213 | 88 | 8 | 8 | 14 | 16 | 28 | 24 | 4 | 19 | 3 |
|  | Point of Sale | 182 |  | 3 | 4 | 1 |  |  | 9 | 180 |  | 3 | 3 |  |  |  | 8 |
|  | Miscellaneous Errors | 2 | 24 | 14 | 114 | 13 | 3 | 2,246 | 16 | 1 | 16 | 10 | 96 | 9 | 2 | 38 | 12 |
|  | Web App Attacks | 4 | 25 | 376 | 32 | 73 | 4 | 148 | 28 | 3 | 11 | 364 | 15 | 61 |  | 13 | 24 |
|  | Crimeware | 5 | 32 | 30 | 54 | 63 | 261 | 5,102 | 14 |  | 5 | 7 | 12 | 1 | 2 | 5 | 1 |
|  | Payment Card Skimmers | 6 |  | 53 |  |  | 1 | 1 | 57 | 5 |  | 44 |  |  |  | 1 | 39 |
|  | Cyber-Espionage |  | 22 | 5 | 2 | 4 | 115 | 112 | 3 |  | 19 | 5 | 1 | 4 | 108 | 98 | 1 |
| Action | Hacking | 176 | 394 | 850 | 84 | 616 | 588 | 958 | 220 | 171 | 43 | 387 | 48 | 89 | 111 | 130 | 30 |
|  | Misuse | 5 | 7 | 48 | 125 | 23 | 13 | 7,417 | 9 | 5 | 5 | 26 | 104 | 13 | 8 | 58 | 6 |
|  | Physical | 12 | 11 | 64 | 73 | 4 | 2 | 18 | 62 | 10 | 2 | 46 | 31 | 2 |  | 11 | 39 |
|  | Social | 9 | 131 | 385 | 37 | 47 | 390 | 147 | 24 | 9 | 32 | 372 | 23 | 37 | 109 | 102 | 20 |
|  | Error | 2 | 28 | 18 | 154 | 16 | 5 | 7,763 | 16 | 1 | 19 | 11 | 119 | 10 | 3 | 47 | 12 |
|  | Malware | 187 | 58 | 395 | 66 | 111 | 358 | 5,219 | 42 | 180 | 26 | 370 | 18 | 42 | 92 | 103 | 24 |
|  | Environmental |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Asset | Server | 185 | 367 | 874 | 184 | 634 | 68 | 880 | 234 | 175 | 34 | 399 | 123 | 101 | 10 | 100 | 38 |
|  | Media | 8 | 12 | 14 | 145 | 6 | 1 | 1,440 | 11 | 7 | 5 | 10 | 105 | 5 | 1 | 31 | 8 |
|  | User Dev | 178 | 43 | 393 | 76 | 50 | 302 | 5,691 | 36 | 174 | 18 | 367 | 25 | 34 | 63 | 109 | 23 |
|  | Person | 10 | 132 | 387 | 41 | 48 | 390 | 149 | 24 | 10 | 33 | 372 | 27 | 38 | 109 | 104 | 20 |
|  | Network |  | 2 | 6 | 3 | 6 |  | 3 |  |  |  | 1 |  | 2 |  | 1 |  |
|  | Kiosk/Terminal | 4 |  | 57 |  |  | 1 | 2 | 57 | 3 |  | 45 |  |  |  | 1 | 38 |
|  | Embedded |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

[5] Verizon 2017 Data Breach Investigations Report

# Appropriate and Expected Practices and Considerations for Today

1. **Robust and Structured Risk Management**
2. **Incorporation into Enterprise Risk Management and Expected Return from Opportunities**
3. **Proactive and Adaptive Risk Identification and Assessment**
4. **Focus on True Trust Boundaries**
5. **Holistic (Internal & Third / Nth Party) Risk Management Coverage**
6. **Adjustment Based on Industry**
7. **Appropriate Reporting**

# Important Practices and Considerations in the Future

1. **Lack of Understanding Considered Risk**
2. **New Core Component (Assurance)**
3. **Zero Trust Information Security Adoption Factor**
4. **Analytics Basis for Risk Management**
5. **Definition and Robust Application of Risk Appetite**
6. **Advanced Risk Reporting and Assignment**
7. **Incorporation and Consideration of Mature Cybersecurity Insurance**

# Example Case – Third Party Information Security Risk

## What's Unique?

- Access to information and assurance
- Varied and unique engagement and risks
- Magnitude of engagement and vendor instances
- Ability to influence change

## Key Points?

- Unique nature requires unique and tailored approach
- Must effectively holistically integrate risk into enterprise risk

# Example Case – End Point Security

## What's Unique?

- Understanding of solution, deployment, and implementation needs
- Alignment with protection scenarios
- Ability to meet changing threats and needs

## Key Points?

- Understanding of all considerations must be factored into assessment
- Changes (e.g. type, frequency) to protected assets important to consider
- Analytical and statistical measures enhance assessment outputs

# Example Case – Information Security Risk Profile

## What's Important?

- Formal and encompassing of all sources of information security risk
- Influence over information security strategy, investment, and protections
- Integration with enterprise risk profile

## Key Points?

- Profile is product of all risk management lifecycle elements (e.g. identification, assessment, management, reporting) and dependent upon effective functions
- Practical use of understanding (assurance) and weights are important and commonly overlooked
- Iterative improvements should be used until a comprehensive risk profile can be produced with little effort

# Apply What You Have Learned Today

**Effective information security risk management is the basis of appropriate information security today and related needs will increase in the future**

**Apply today's messages:**

- **Immediately:** Review your organization's information security risk management practices and identify opportunities for incorporation of today's messages
- **Near-Term Actions:**
  - Review and challenge how your organization handles core risk management challenges (measurement and management)
  - Create a roadmap to implement and maintain risk management practices practical for your organization and appropriate for today and the future