Cyber Risk Quantification: Translating technical risks into business terms

Jesper Sachmann
RSA Denmark

13-06-2018
CYBER RISK QUANTIFICATION:

TRANSLATING TECHNICAL RISKS INTO
BUSINESS TERMS

Jesper Sachmann GRCP GRCA

Atos Cyber Security Day
June 13, 2018
IF YOUR CEO ASKED YOU...

How much risk do we have?
How much less risk will we have if...?

How would you answer?
THE COMMUNICATION CHALLENGE

CFO
“How much risk do we have? Are we spending too little or too much on mitigation?”

AUDIT
“Did you fix those high priority issues?”

BOARD/CEO
“We don’t want to be the next news headline cybercrime victims. Are we doing enough to minimize risk?”

CIO
“Are we spending our cybersecurity budget on the right things? What is the ROI?”

CISO
“Εχουμε πάνω από δέκα χιλιάδες τρωτά σημεία, είναι συμβατό με το ογδόντα τοις εκατό”
BALD TIRE

How much risk?
THERE WILL ALWAYS BE ASSUMPTIONS IN ANY ANALYSIS.

THE KEY IS TO SURFACE THEM.
The way most cybersecurity professionals measure risk today fails to quantify cyber risk in terms the business can understand and use.
## SIDE EFFECT OF THE QUALITATIVE APPROACH
### WHICH ONE DESERVES MORE ATTENTION?

<table>
<thead>
<tr>
<th>Table Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Access To Confidential Data</td>
<td>Operational fraud, loss of intellectual property, and loss of customers from damaged reputation resulting from an access control breach</td>
</tr>
<tr>
<td>Executive Sponsorship</td>
<td>The organization lacks an executive management sponsor for risk management leading to poor visibility at the business and corporate management level.</td>
</tr>
<tr>
<td>Least Privilege</td>
<td>The concept of Least Privilege is not used leading to over-authorization of users’ roles or access to data, transactions or business systems.</td>
</tr>
<tr>
<td>Performance and Capacity Management</td>
<td>The organization does not have a strategy including application performance and infrastructure utilization planning to properly make use of, and plan accordingly, IT resources resulting in IT resource (application and infrastructure) instability, cost overruns, increased operational maintenance and support costs, under-utilized resources and financial impacts.</td>
</tr>
<tr>
<td>Technology Documentation</td>
<td>The IT organization does not properly document and communicate the use and operation of IT resources (applications, infrastructure, etc.) resulting in poor end user experiences, increased support costs, increased help desk incidents and uninformed maintenance and operations support personnel.</td>
</tr>
<tr>
<td>Bodily Injury due to slips and falls</td>
<td>Loss of employee productivity and injury / possible litigation or workers compensation claims from employees, or from customers or others on-premises.</td>
</tr>
</tbody>
</table>

Can you compare them? How can you take a decision based on this report?
THE RISK LANDSCAPE IN A NUTSHELL...

Complex

Dynamic

Limited Resources

Which means...
ORGANIZATIONS MUST EXCEL AT **PRIORITIZING** THEIR CYBER RISK PROBLEMS AND SOLUTIONS.
PRIORITIZATION REQUIRES...

Comparing their various concerns and solution options, which requires...

Measurement
THE RISK MANAGEMENT STACK

Effective Risk Management enabled by well-informed decisions.

Comparisons require measurements.

Measurements require a risk model.

Business-Driven Security
### CYBER RISK RELEVANCE IS ON THE RISE
THE TOP 10 OPERATIONAL RISK RANKING FOR 2018 OF

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>2018 position</th>
<th>2017 position</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT disruption</td>
<td>1</td>
<td>1*</td>
<td></td>
</tr>
<tr>
<td>Data compromise</td>
<td>2</td>
<td>1*</td>
<td></td>
</tr>
<tr>
<td>Regulatory risk</td>
<td>3</td>
<td>2</td>
<td>↓</td>
</tr>
<tr>
<td>Theft and fraud</td>
<td>4</td>
<td>9</td>
<td>↑</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>5</td>
<td>3</td>
<td>↓</td>
</tr>
<tr>
<td>Mis-selling</td>
<td>6</td>
<td>5**</td>
<td>↓</td>
</tr>
<tr>
<td>Talent risk</td>
<td>7</td>
<td>new</td>
<td></td>
</tr>
<tr>
<td>Organisational change</td>
<td>8</td>
<td>6</td>
<td>↓</td>
</tr>
<tr>
<td>Unauthorised trading</td>
<td>9</td>
<td>5**</td>
<td>↓</td>
</tr>
<tr>
<td><strong>Model risk</strong></td>
<td>New Entry</td>
<td>10</td>
<td>↑</td>
</tr>
</tbody>
</table>
IN A TYPICAL ORGANIZATION, 70% TO 90% OF “HIGH RISK” ISSUES, AREN’T

Why?
Which Of These Are **Risks**?

Typical Top 10 Risk List

- POINT OF SALE ATTACKS
- CLOUD COMPUTING
- INSIDER THREAT(S)
- CYBER CRIMINALS
- APPLICATION VULNERABILITIES
- HACKTIVISTS
- PHISHING / SOCIAL ENGINEERING
- THIRD-PARTY RISK
- MOBILE MALWARE
- BUSINESS CONTINUITY
NONE OF THESE ARE RISKS!

APPLICATION VULNERABILITIES ➔ CONTROL DEFIC.
CLOUD COMPUTING ➔ ASSET
INSIDER THREAT(S) ➔ THREAT
PHISHING / SOCIAL ENGINEERING ➔ METHOD

WE CAN ONLY ASSESS THE RISK OF LOSS EVENTS

<table>
<thead>
<tr>
<th>INSIDER THREAT(S)</th>
<th>“LOSS OF AVAILABILITY OF SYSTEMS DUE TO MALICIOUS INSIDER”</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATION VULNERABILITIES</td>
<td>“THEFT OF CUSTOMER PII DATA THROUGH APPLICATION ATTACKS”</td>
</tr>
</tbody>
</table>
FACTOR ANALYSIS OF INFORMATION RISK (FAIR) OVERVIEW
A "FAIR DEFINITION" OF RISK
FAIR – FACTOR ANALYSIS FOR INFORMATION RISK

The RISK is

- **the probable frequency** and **probable magnitude** of future loss (*)

- Risk is a derived (calculated) value
- To address the inherent uncertainty of risk, probabilistic distributions are used
- The risk is defined in terms of "financial loss exposure"

(*) associated with a specific event
FAIR: THE ANALYTICS MODEL

Frequency (#)

Risk (€)

Loss Event Frequency

Threat Event Frequency

Contact Frequency

Probability of Action

Threat Capability

Resistance Strength

Vulnerability

Primary Loss

Secondary Risk

Secondary Loss Event Frequency

Secondary Loss Magnitude

Accredited as an Industry Standard by

Complementary to Risk Frameworks

Supported by a Fast Growing Community

FAIR Book Inducted in Cybersecurity Canon
**FAIR: THE METHODOLOGY**

1. **Scope the scenarios**

   - **Risk Scenario**
     - Threat
     - Assets
     - Effect
     - Controls

2. **Gather Data**: use available data or estimate the ranges for the risk factors
   - SCALE: chose the level to work at

3. **Run the FAIR model**: apply the calculations
   - Manual or Automatic (more efficient)

4. **Reporting**
THE OUTCOME: WHAT YOU GET

CYBER RISK IS EXPRESSED IN FINANCIAL TERMS:

“HOW MUCH RISK DO WE HAVE?”

Maximum $1.3B
90th % $405.3M
Average $226.5M
10th % $112.9M
Minimum $31.3M
Risk Appetite $130.0M

“WHAT ARE OUR TOP RISKS?”

Now you can answer many more questions!

“HAVE WE REDUCED RISK?”

“WHAT TYPE OF LOSS CAN WE EXPECT?”

Productivity
Replacement
Primary Response
Fines and Judgments
Reputation
Secondary Response

$7.3M
$671
$100K
$1.3M
$7.6M
$1.4M

$0
$20K
$40K
$60K
$80K
$100K
$120K
$140K
RSA ARCHER CYBER RISK QUANTIFICATION

Key Features

• Built-in risk calibration and analysis engine for cyber risk calculation
• Templated workflow for easy scenario modeling
• On-demand risk analytics for answers to questions on the fly
• Mathematical simulations to build your risk profile with limited data
• Existing loss tables based on industry data
• Easy-to-use SaaS application
• User-friendly interface
Cyber Risk Quantification

- Cyber Incident & Breach Response
- IT Security Vulnerabilities Program
- IT Regulatory Management
- PCI Management
- Information Security Management System (ISMS)

**NOTE:** the "Cyber Risk Quantification" use case is powered in the backend by the RiskLens tool which is a (SaaS) product integrated with RSA Archer.
RSA PORTFOLIO

Unified Security Analytics
SECURITY ANALYTICS FOR:
- LOGS
- PACKETS
- ENDPOINT
- SECOPS MANAGER

Secure Access, No Boundaries
- ACCESS MANAGEMENT
- IDENTITY
- GOVERNANCE & LIFECYCLE

Centralized, Omni-Channel Fraud
- WEB THREAT DETECTION
- ADAPTIVE AUTHENTICATION
- ADAPTIVE AUTHENTICATION FOR eCOMMERCE
- FRAUD ACTION

Proven Business Risk Management
- IT SECURITY & RISK MANAGEMENT
- ENT & OPERATIONAL RISK MANAGEMENT
- 3RD PARTY GOVERNANCE
- BUSINESS RESILIENCY
- PUBLIC SECTOR
- AUDIT MANAGEMENT
- REG & CORP COMPLIANCE

Advancing your Risk and Security Maturity
- ADVANCED RISK AND CYBERSECURITY CONSULTING SERVICES
- INCIDENT RESPONSE
- DESIGN AND IMPLEMENTATION
- CUSTOMER SUPPORT
- EDUCATION SERVICES

RSA CYBER ANALYTICS PLATFORM
RSA CUSTOMER LEADERSHIP

30,000+ customers

50+ million identities

1 billion consumers

97%

20 of the
TOP 20

Manufacturing

Consumer product

Financial institutions

Healthcare institutions

Transportation

94%

19 of the
TOP 20

18 of the TOP 20 Telecom

16 of the TOP 20 Energy

10 of the TOP 10 Technology

13 of the 15 Executive Departments of U.S. Government

All branches of US Military
RSA INDUSTRY LEADERSHIP

$60+ billion
Value of transactions protected per year

$8+ billion
Value of fraudulent losses prevented per year

97%
Of malicious sites blocked in less than 30 minutes

1+ million
Advanced attacks detected and stopped

95~
Fraud detection rates

6
Gartner Leaders quadrants

400,000+
Malware samples analyzed per week

Phishing attack identified every 30 seconds

~510 issued patents
~240 pending patents
across current product portfolio

~510 issued patents
~240 pending patents
across current product portfolio

4M
Indicators of compromise actively maintained in RSA Live Threat Intelligence

Leaders quadrants

Technology Awards

GSN Homeland Security Award 2015