Adventures in Cyberspace

SECURITY STRATEGIEN IM GOLBALEN SPANNUNGSFELD

IT-SeCX St. Pölten 2014
Robert Lamprecht
CONTENTS

1. WHY CYBER
2. THREAT ACTORS
3. ORGANISATIONAL POSTURE
4. SECURITY FRAMEWORKS
5. SECURITY OFFERINGS
6. GOVERNMENT RESPONSE
7. SECURITY RESPONSE
8. FORESIGHT
WHY CYBER?

HYPERCONNECTIVITY
THE INTERNET OF THINGS
INFORMATION AVAILABILITY
ANYTIME ANY PLACE
SCALEABILITY
ON-DEMAND
Why Cyber?

Cyberspace designed for information sharing
Largely anonymous
May not know you have been targeted
Attribution is not straightforward

Hyperconnectivity
The Internet of Things
Information availability
Anytime anywhere
Scaleability
On-demand

Privacy

Cyber?
Revealed by Whistleblower Edward Snowden in June 2013

Global surveillance of telecommunications and internet without prior suspicions or legal basis

Since at least 2007 by intelligence agencies NSA (USA) and GCHQ (UK)

Participation of intelligence agencies in Australia, Canada and New Zealand → together they form the so-called Five Eyes
Program for surveillance and analysis of electronic media and electronically recorded data.

Surveillance of people within and outside of the USA. Private citizens as well as governments.

Participation by many large internet and technology companies in the USA – Microsoft, Google, Facebook, Apple, Yahoo, etc.

“You need the haystack to find the needle” – Keith Alexander (former NSA director)

PRISM Program Cost: ~ $20M per year
CONTENTS

1. WHY CYBER
2. THREAT ACTORS
3. ORGANISATIONAL POSTURE
4. SECURITY FRAMEWORKS
5. SECURITY OFFERINGS
6. GOVERNMENT RESPONSE
7. SECURITY RESPONSE
8. FORESIGHT
SO WHAT’S THE PROBLEM?

CYBERSPACE AND THE INTERNET

COMPANIES

INDIVIDUALS

GOVERNMENTS

NATIONAL INFRASTRUCTURE

THREAT ACTORS
WHO IS BEING TARGETED?

What Industries?
WHO IS BEING TARGETED?

AUTOMOTIVE  AEROSPACE  ENERGY PROVIDERS  RETAIL BANKS  PROFESSIONAL & LEGAL SERVICES

DEFENCE  ADVANCED MANUFACTURING  RENEWABLE ENERGY  INVESTMENT BANKS  RESEARCH INSTITUTES

PHARMACEUTICALS & BIOTECHNOLOGY  MINING & NATURAL RESOURCES  COMMUNICATIONS  WIDER FINANCIAL SERVICES  ACADEMIA
RECENT ATTACKS

Late 2013: Security breach at Target (USA). Theft of 98 million user accounts, thereof 40 million credit card data over a period of 3 weeks.

Early 2014: Details of more than 2000 user accounts of Tesco.com (USA) were published on the internet.

September 2014: Notification of the public about the theft of the credit card data of 56 million customers
WHO ARE THEY?
WHY DO THEY DO IT?
THE THREAT
ACTORS
THE THREAT ACTORS

1. **Hacktivism**
   - **Motivation:** Hacking inspired by ideology
   - **Impact to Business:** Public distribution, reputation loss

2. **Organised Crime**
   - **Motivation:** Financial advantage
   - **Impact to Business:** Theft of information

3. **The Insider**
   - **Motivation:** Grudge, financial gain
   - **Impact to Business:** Distribution or destruction, theft of information, reputation loss

4. **State-Sponsored**
   - **Motivation:** Espionage and sabotage
   - **Impact to Business:** Disruption or destruction, theft of information, reputational loss
WHAT IS BEING STOLEN?

INFORMATION THAT IS VALUABLE
- Intellectual Property
- Business Processes
- Customer, Supplier and Personnel Data

BUSINESS CRITICAL INFORMATION
- Financials
- Business Plans
- New Products
- New Markets

CRITICAL BUSINESS TRANSACTIONS
- Raising Finance
- JV
- M&A
- Divestitures
The Fraud Triangle

- **Rationale**
- **Opportunity**
- **Motivation**
- **Management Override**

Fraud Triangle

Fraud Diamond
PROFILE OF A FRAUDSTER

TRADITIONAL PROFILE
• 70 percent of fraudster are between the ages of 36 and 55
• 61 percent are employed by the victim organization – of these, 41 percent for more than 6 years
• In 70 percent of frauds, the perpetrator colluded with others
• 72 percent of frauds were perpetrated over a one-to-five year period
• The most prevalent fraud is misappropriation of assets (56 percent)

MODERN PROFILE
• Predominantly unknown outsiders
• Employees of the victim department
• Customers
• Other business associates
• Division or department managers
• Service providers
• Employees of another department
• General manager
CONTENTS

1. WHY CYBER
2. THREAT ACTORS
3. ORGANISATIONAL POSTURE
4. SECURITY FRAMEWORKS
5. SECURITY OFFERINGS
6. GOVERNMENT RESPONSE
7. SECURITY RESPONSE
8. FORESIGHT
HOW MUCH DOES IT ALL MATTER?

IMPACT
Financial
Reputational

THREAT
Who would target us and why?

ASSETS
What are we trying to protect?

CAN WE ACCEPT THE RISK?
HOW MUCH ARE WE PREPARED TO SPEND TO MITIGATE IT?

- FINANCIAL PERFORMANCE
- COMPETITIVE ADVANTAGE
- REPUTATION
- MARKET PRESENCE
## Changes in Risk Ranking 2011 → 2013

<table>
<thead>
<tr>
<th>2011 Rank</th>
<th>Risk Description</th>
<th>2013 Rank</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Loss of customers/cancelled orders</td>
<td>1</td>
<td>Loss of customers/cancelled orders</td>
</tr>
<tr>
<td>2</td>
<td>Talent and skills shortage</td>
<td>2</td>
<td>High taxation</td>
</tr>
<tr>
<td>3</td>
<td>Reputational risk</td>
<td>3</td>
<td>Cyber risk</td>
</tr>
<tr>
<td>4</td>
<td>Currency fluctuation</td>
<td>4</td>
<td>Price of material inputs</td>
</tr>
<tr>
<td>5</td>
<td>Changing legislation</td>
<td>5</td>
<td>Excessively strict regulation</td>
</tr>
<tr>
<td>6</td>
<td>Cost and availability of credit</td>
<td>6</td>
<td>Changing legislation</td>
</tr>
<tr>
<td>7</td>
<td>Price of material inputs</td>
<td>7</td>
<td>Inflation</td>
</tr>
<tr>
<td>8</td>
<td>Inflation</td>
<td>8</td>
<td>Cost and availability of credit</td>
</tr>
<tr>
<td>9</td>
<td>Corporate liability</td>
<td>9</td>
<td>Rapid technological changes</td>
</tr>
<tr>
<td>10</td>
<td>Excessively strict regulation</td>
<td>10</td>
<td>Interest rate changes</td>
</tr>
</tbody>
</table>

How Much is Your Hacked Data Worth?  Black market $ prices

- CVV 3-digit security code: $2
- Bank a/c details: 5
- Credit card (market flooded): 10
- Full package of identifying info (name, DOB etc): 3
- Credit card (old): 5
- Health credentials used to buy drugs, or make fake insurance claims: 10
- PayPal / eBay account: 27
- Credit card (fresh): 45

lowest ............................................................... average ................................................ highest
WHAT WE SEE IN LARGE COMPLEX ENVIRONMENTS
CONTENTS

1. WHY CYBER
2. THREAT ACTORS
3. ORGANISATIONAL POSTURE
4. SECURITY FRAMEWORKS
5. SECURITY OFFERINGS
6. GOVERNMENT RESPONSE
7. SECURITY RESPONSE
8. FORESIGHT
SECURITY FRAMEWORKS: BUILDING SECURITY CAPABILITY ON STRONG FOUNDATIONS
SECURITY FRAMEWORKS: NIST CYBER SECURITY FRAMEWORK

IDENTIFY
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT
- Access Control
- Awareness & Training
- Data Security
- Information Protection Process & Procedures
- Maintenance
- Protective Technology

DETECT
- Anomalies & Events
- Security Continuous Monitoring
- Detection Processes

RESPOND
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER
- Recovery Planning
- Improvements
- Communication
CONTENTS

1. WHY CYBER
2. THREAT ACTORS
3. ORGANISATIONAL POSTURE
4. SECURITY FRAMEWORKS
5. SECURITY OFFERINGS
6. GOVERNMENT RESPONSE
7. SECURITY RESPONSE
8. FORESIGHT
Cyber Risk in the Boardroom

- Board-level Threat Briefing
- Board-level Impact Analysis
- Planning for the Future

Cyber Maturity Assessment

- Review of information asset protection
- Maturity of approach
- Preparedness against cyber attack.

Security Transformation

- Security Strategy and Governance
- Security Programme Management
- Security Policies, Processes and Standards

A COMPREHENSIVE SECURITY OFFERING
# CYBER RISK IN THE BOARDROOM

## PHASE 1: THREAT BRIEFING

**Objectives & Benefits**
- to equip board members with a clear jargon-free explanation of the threat.
- an understanding of the risk to their organisation.
- to equip board members with a clear indication of how the cyber threat could impact their business.
- Build and understanding of how particular business activities affect the overall risk profile for the business.
- To build out a set of options for the client to challenge and inform the board’s view of how managing cyber risk effectively can benefit the business in the long term.

**Key activities**
- Determine key threat actors
- Analyse and assess capability and motivations of threats
- Define threat model
- Provide examples of similar threat actors and likely impact

**Deliverables**
- A report identifying areas of particular focus, specific threat actors, likely information and systems that would be targeted.
- Discussion with Board members and other senior executives to improve awareness and understanding of the subject.

## PHASE 2: IMPACT ANALYSIS

**Objectives & Benefits**
- to equip board members with a clear indication of how the cyber threat could impact their business.
- Build and understanding of how particular business activities affect the overall risk profile for the business.

**Key activities**
- Identify key business processes and assets
- Overview of business impact assessment
- Model key risk scenarios based upon available open-source reporting.

**Deliverables**
- A report identifying particular business areas that could be affected by specific threats.
- Discussion with Board members and other senior executives to improve awareness and understanding of the subject.

## PHASE 3: PLANNING FOR THE FUTURE

**Objectives & Benefits**
- Summarize previous discussions and align with leading industry practice
- Discussion with Board members to identify and agree future business posture and operating models.
- Define a board approach to risk management

**Key activities**
- A report highlighting a number options the board to consider taking into account:
  - Risk appetite, business growth plans, incident management.
  - Final discussion on next steps

**Deliverables**
- A report identifying areas of particular focus, specific threat actors, likely information and systems that would be targeted.
- Discussion with Board members and other senior executives to improve awareness and understanding of the subject.

## Timeline

<table>
<thead>
<tr>
<th>Week 1</th>
<th>Week 2</th>
<th>Week 3</th>
<th>Week 4</th>
<th>Week 5</th>
<th>Week 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board Meeting</td>
<td>Board Meeting</td>
<td></td>
<td>Board Meeting</td>
<td></td>
<td>Board Meeting</td>
</tr>
</tbody>
</table>
THE GOVERNMENT RESPONSE

1. TACKLING CYBER CRIME and making the UK one of the most secure places in the world to do business.

2. Making the UK more RESILIENT TO CYBER ATTACK and better able to protect our interests in cyberspace.

3. Helping to shape an OPEN, VIBRANT AND STABLE CYBERSPACE which the UK public can use safely and that supports open societies.

4. Building the UK’s cross-cutting KNOWLEDGE, SKILLS AND CAPABILITY to underpin all cyber security objectives.
TEN STEPS TO CYBER MATURITY

HOME AND MOBILE NETWORKING
Develop a mobile working policy & train staff to adhere to it. Apply the secure baseline build to all devices. Protect data at all times.

NETWORK SECURITY
Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access & malicious content. Monitor & test security controls.

MALWARE PROTECTION
Produce relevant policy & establish anti-malware defences that are applicable & relevant to all business areas. Scan for malware across the organisation.

SECURE CONFIGURATION
Apply security patches & ensure that the secure configuration of all ICT systems is maintained. Create a system inventory & define a baseline build for all ICT devices.

MONITORING
Establish a monitoring strategy & produce supporting policies. Continuously monitor all ICT systems & networks. Analyse logs for unusual activity that could indicate an attack.

REMOVABLE MEDIA CONTROLS
Produce a policy to control all access to removable media. Limit media types & use. Scan all media for malware before importing onto corporate systems.

MANAGING USER PRIVILEGES
Establish account management processes & limit the number of privileged accounts. Limit user privileges & monitor user activity. Control access to activity & audit logs.

INCIDENT MANAGEMENT
Establish an incident response & disaster recovery capability. Produce & test incident management plans. Provide specialist training to the incident management team.

USER EDUCATION AND AWARENESS
Produce user security policies covering acceptable & secure use of the organisation’s systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

INFORMATION RISK MANAGEMENT REGIME
Establish an effective governance structure and determine your risk appetite – just like you would for any other risk. Maintain the Board’s engagement with the cyber risk. Produce supporting IRM policies.

Source: CESG – 10 steps to Cyber Maturity
HOW DO YOU SEE THE CYBER RISK TO THE BUSINESS? (Austria)
1. WHY CYBER
2. THREAT ACTORS
3. ORGANISATIONAL POSTURE
4. SECURITY FRAMEWORKS
5. SECURITY OFFERINGS
6. GOVERNMENT RESPONSE
7. SECURITY RESPONSE
8. FORESIGHT
ACHIEVING & DISPLAYING POTENTIAL
REPUTATION & SOCIAL MEDIA

Governance
• Understand your social media assets
• Understand the benefits and risks with social media

Compliance
• Financial Information disclosure
• Advertising and promotion
• Human Resources

Processes & Policies
• Ownership of social media assets
• Security procedures (e.g. passwords)

Reputation
• Monitor media channels
• Manage your response

PR Crisis
• Prepare and rehearse

Training
• Training staff
• Coaching the board
RESILIENCE

**Identify Risks**
- Short and long-term thinking; horizon scanning, emerging risks

**Analyse & Prioritise**
- Impact assessment; risk quantification; prioritisation

**Risk Response**
- Mitigation planning and delivery

**Incident Planning**
- Business continuity; disaster recovery; cyber response

**Exercise & Training**
- Crisis simulation; skills and capability improvement

**Governance & Assurance**
- Policies and standards; audit & assurance
THREAT INTELLIGENCE AND DETECTION

Management Information
• Customer trends and performance statistics

Market Intelligence
• Market innovations and competence

Threat Intelligence
• Identify threats to future growth

Ability to seize an opportunity denied to competition because a better informed view of the management of risk is taken.

Opportunity management whereby a detailed evaluation is undertaken of new business opportunities before deciding to take the opportunity.

Achieving a positive outcome from a situation that could have gone wrong without effective judgement/risk management.
WORKING TOGETHER AND SHARING INSIGHTS

With Customers
• Delivering brand confidence and value through investment in digital proposition and other brands.
• Effective communication of security commitment and highlight customers’ obligations.

With Peers and Advisors
• Build strength in numbers, learning from other experiences, industry exercises
• Public/Private Information Sharing Groups
SPEED AND AGILITY

Preparation
• To handle incidents: skilled teams, procedures e.g. media handling
• To prevent incidents: risk management, security technology, user training

Detection and Analysis
• Know your likely attackers
• Identify signs of an incident: precursors and indicators
• Incident Analysis
• Prioritisation: Impact analysis and recovery
• Communication: Internal and external

Containment, Eradication & Recovery
• Type of incident and necessary response e.g. Evidence gathering
• Identification of all affected areas
• Document response measures

Post-Incident Activity
• Lessons learned
• What can you share with the community?
PROTECTION

Reputation and Social Media
• Optimise the use of online media channels and technologies

Resilience and Business Protection
• Preparation and response measures

Threat Intelligence and Detection
• Anticipate changes in the threat landscape

Working Together and Sharing Insights
• Beneficial sharing of knowledge and pooling of resources

Speed and Agility
• Response to incidents and regulation

Protect Customer Confidence
Protect Brand and Regulatory Confidence
Protect Shareholder Confidence
### Automation of Personal Banking
Cost efficiency will lead to sophisticated data mining and service through apps.

### Companies will protect only crown jewels
Increased sophistication of threat actors will mean the internet becomes a more hostile environment.

### Everything will be an App
Seduced by the simplicity that apps offer. The growing dominance of mobile computing.

### Banks will do more than manage money
Commoditisation will force banks to diversify e.g. Identity broker, trusted marketplace, eWallet.

### Attackers will be too fast for human response
Future intruders will be human guided AI worms which will require some level of AI management and response.

### Balkanisation of the Internet
Nations applying their own protective measures to elements of the internet that leads to fragmentation.

### Internet Outages for Material Length of Time
Cascading technology failures or Militarisation leads to online warfare.