CYBER ATTACKS AND DATA PRIVACY AND DATA PROTECTION (GDPR) ON BANKING SYSTEMS

THE IMPACT ON THE BANK INDUSTRY

Supakorn Kungpisdan, Ph.D.

CISSP, CISA, CISM, PECB ISO 27001 PI, IRCA ISO27001 PA, PECB ISO 22301 PI, PECB ISO31000 RM, Security+, ITIL Foundation, C|CISO, E|CSA, C|EH, C|HFI, E|NSA, E|CES, C|EI, C|SCU, CCNA Instructor, CCNAS Instructor

Managing Director, Alpha Wolf

AGENDA

- R V CONNEX INTRODUCTION
- CYBER RISKS AND ATTACKS ON FINANCIAL INDUSTRY
- GDPR AND CYBERSECURITY

RVC CAPABILITIES

- SYSTEM INTEGRATION / SOFTWARE DEVELOPMENT
- UNMANNED AIRCRAFT SYSTEM: UAS
- AIRCRAFT AVIONIC SERVICES AND AIRCRAFT MODIFICATION SERVICE
- CYBER
- SATELLITES AND GROUND STATION

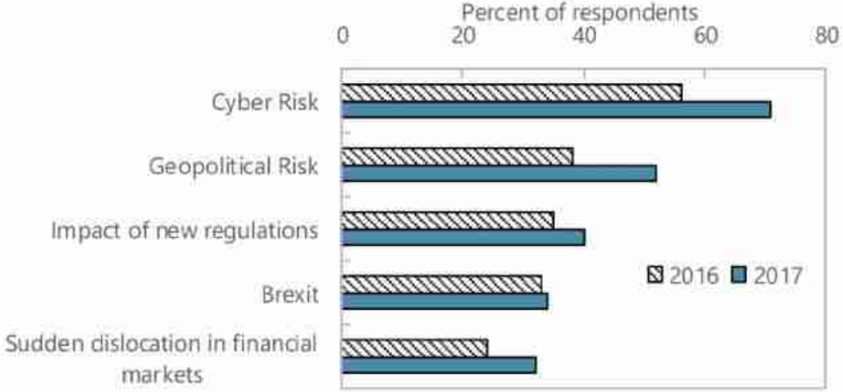
CYBER RISKS AND ATTACKS

ON FINANCIAL INDUSTRY

R V CONNEX

Cyber risk can be defined as "*operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems*"

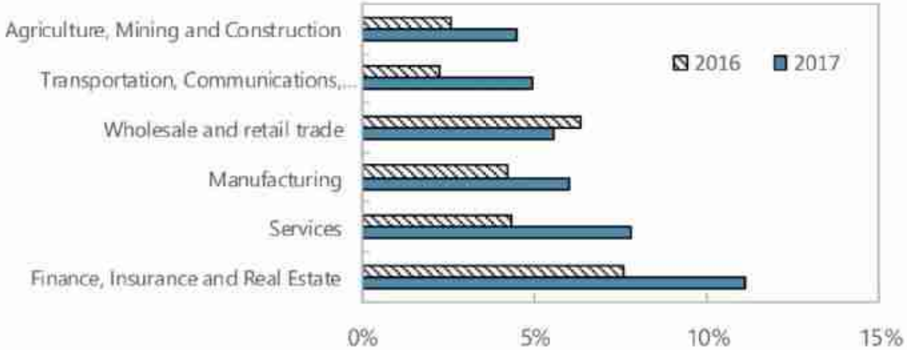
Risk to broader economy



Source: DTCC Systemic Risk barometer 2017Q1

Cyber risk awareness by sectors in the U.S.

(share of annual reports featuring "cyber-attack")



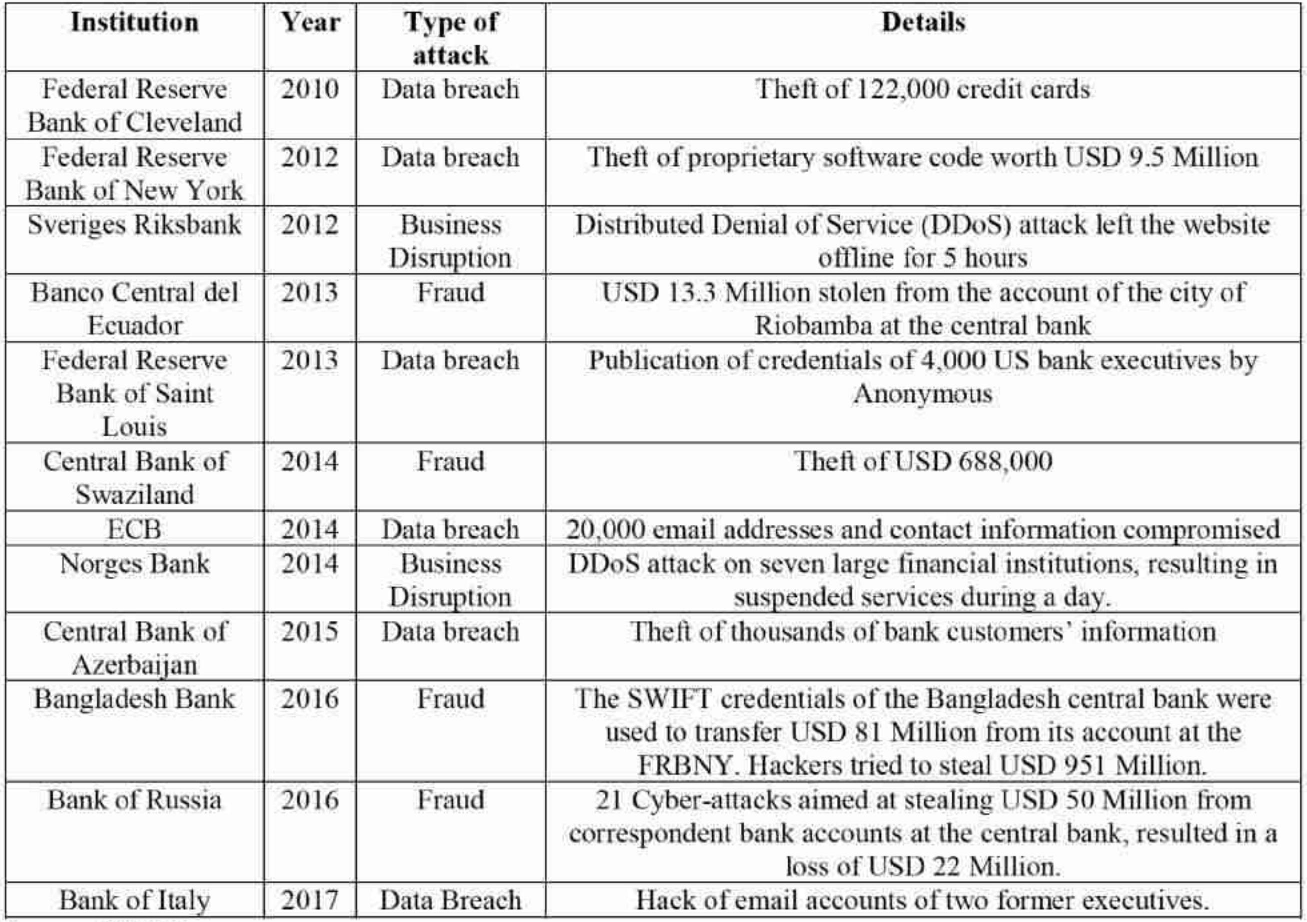
Sources: SEC form 10-K; and staff calculations.

REF: IMF Working Paper

Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

RV CONNEX

ATTACKS ON CENTRAL BANKS



Institution	Year	Type of attack	Details
Federal Reserve Bank of Cleveland	2010	Data breach	Theft of 122,000 credit cards
Federal Reserve Bank of New York	2012	Data breach	Theft of proprietary software code worth USD 9.5 Million
Sveriges Riksbank	2012	Business Disruption	Distributed Denial of Service (DDoS) attack left the website offline for 5 hours
Banco Central del Ecuador	2013	Fraud	USD 13.3 Million stolen from the account of the city of Riobamba at the central bank
Federal Reserve Bank of Saint Louis	2013	Data breach	Publication of credentials of 4,000 US bank executives by Anonymous
Central Bank of Swaziland	2014	Fraud	Theft of USD 688,000
ECB	2014	Data breach	20,000 email addresses and contact information compromised
Norges Bank	2014	Business Disruption	DDoS attack on seven large financial institutions, resulting in suspended services during a day.
Central Bank of Azerbaijan	2015	Data breach	Theft of thousands of bank customers' information
Bangladesh Bank	2016	Fraud	The SWIFT credentials of the Bangladesh central bank were used to transfer USD 81 Million from its account at the FRBNY. Hackers tried to steal USD 951 Million.
Bank of Russia	2016	Fraud	21 Cyber-attacks aimed at stealing USD 50 Million from correspondent bank accounts at the central bank, resulted in a loss of USD 22 Million.
Bank of Italy	2017	Data Breach	Hack of email accounts of two former executives.

Source: ORX News

REF: IMF Working Paper

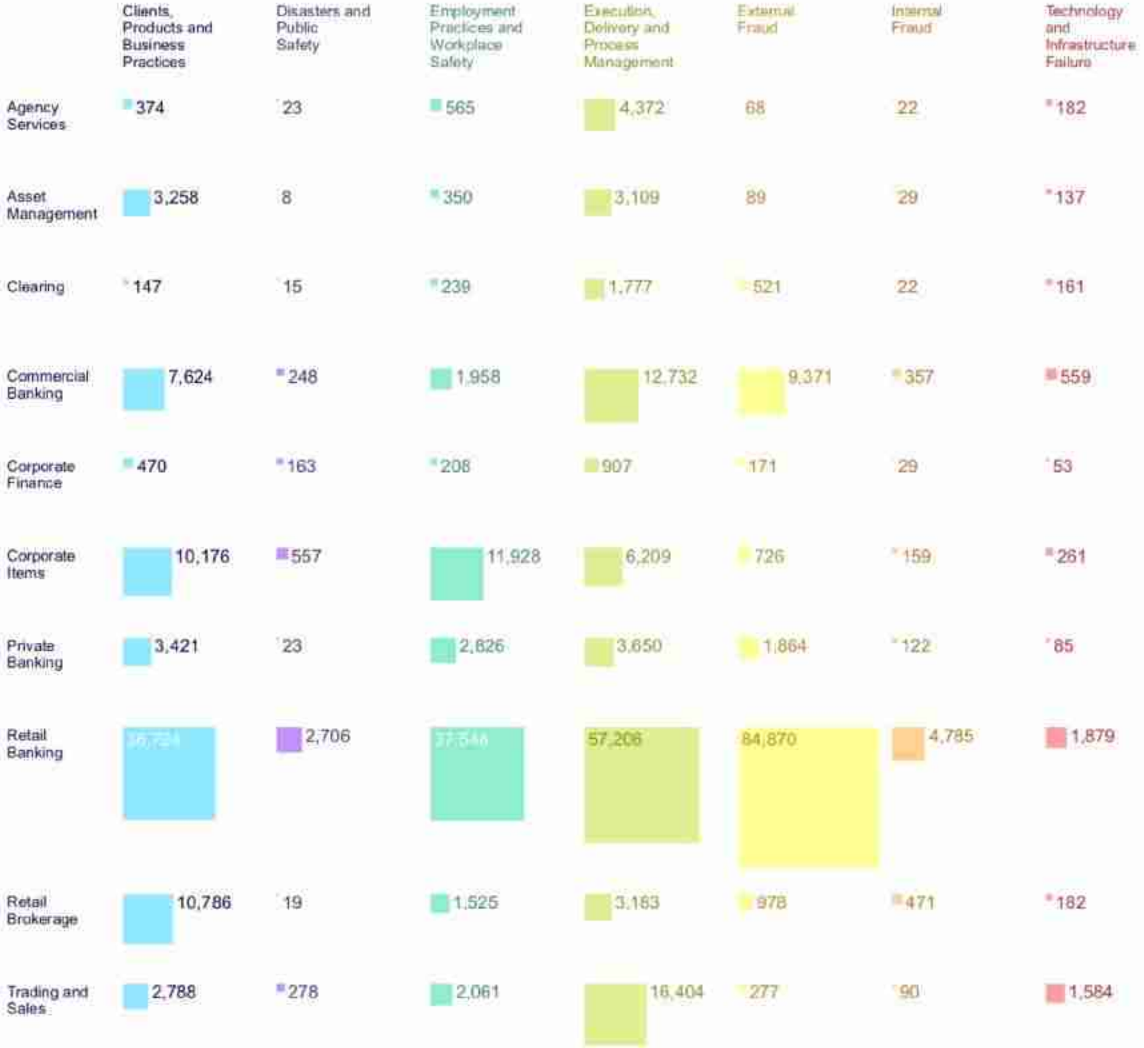
Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

€170bn

This was the global industry loss between 2012 and 2017, from a reported total of 358,669 loss events.

REF: Annual Banking Loss Report
Operational risk loss data for banks submitted between 2012 and 2017
June 2018
https://managingrisktogether.orx.org/sites/default/files/downloads/2018/09/annualbankinglossreport2018-printversion.pdf

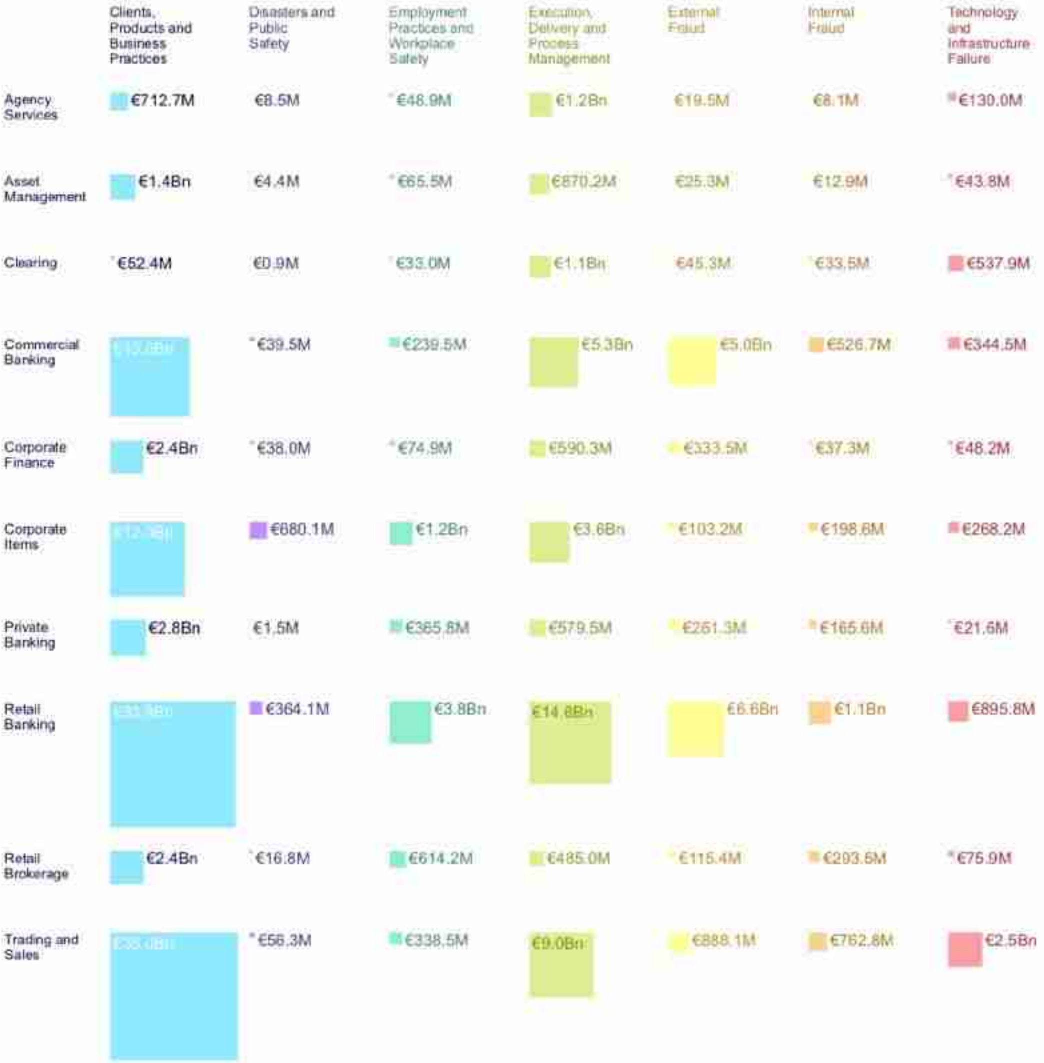
THE NUMBER OF EVENTS SUBMITTED IN EACH BUSINESS LINE AND EVENT TYPE BETWEEN 2012 AND 2017



	Clients, Products and Business Practices	Disasters and Public Safety	Employment Practices and Workplace Safety	Execution, Delivery and Process Management	External Fraud	Internal Fraud	Technology and Infrastructure Failure
Agency Services	374	23	565	4,372	68	22	182
Asset Management	3,258	8	350	3,109	89	29	137
Clearing	147	15	239	1,777	521	22	161
Commercial Banking	7,624	248	1,958	12,732	9,371	357	559
Corporate Finance	470	163	208	907	171	29	53
Corporate Items	10,176	557	11,928	6,209	726	159	261
Private Banking	3,421	23	2,826	3,650	1,864	122	85
Retail Banking	36,724	2,706	37,548	57,206	84,870	4,785	1,879
Retail Brokerage	10,786	19	1,525	3,183	978	471	182
Trading and Sales	2,788	278	2,061	16,404	277	90	1,584

REF: Annual Banking Loss Report
Operational risk loss data for banks submitted between 2012 and 2017
June 2018

THE TOTAL LOSS SUBMITTED IN EACH BUSINESS LINE AND EVENT TYPE BETWEEN 2012 AND 2017



	Clients, Products and Business Practices	Disasters and Public Safety	Employment Practices and Workplace Safety	Execution, Delivery and Process Management	External Fraud	Internal Fraud	Technology and Infrastructure Failure
Agency Services	€712.7M	€8.5M	€48.9M	€1.2Bn	€19.5M	€8.1M	€130.0M
Asset Management	€1.4Bn	€4.4M	€65.5M	€870.2M	€25.3M	€12.9M	€43.8M
Clearing	€52.4M	€0.9M	€33.0M	€1.1Bn	€45.3M	€33.5M	€537.9M
Commercial Banking	[illegible]	€39.5M	€239.5M	€5.3Bn	€5.0Bn	€526.7M	€344.5M
Corporate Finance	€2.4Bn	€38.0M	€74.9M	€590.3M	€333.5M	€37.3M	€48.2M
Corporate Items	[illegible]	€680.1M	€1.2Bn	€3.6Bn	€103.2M	€198.6M	€268.2M
Private Banking	€2.8Bn	€1.5M	€365.8M	€579.5M	€261.3M	€165.6M	€21.6M
Retail Banking	[illegible]	€364.1M	€3.8Bn	€14.8Bn	€6.6Bn	€1.1Bn	€895.8M
Retail Brokerage	€2.4Bn	€16.8M	€614.2M	€485.0M	€115.4M	€293.6M	€75.9M
Trading and Sales	[illegible]	€56.3M	€338.5M	€9.0Bn	€888.1M	€762.8M	€2.5Bn

REF: Annual Banking Loss Report
Operational risk loss data for banks submitted between 2012 and 2017
June 2018

North America

Frequency: 19,297 ▼ (20,971)
Total loss: €3.9Bn ▼ (€13.2bn)

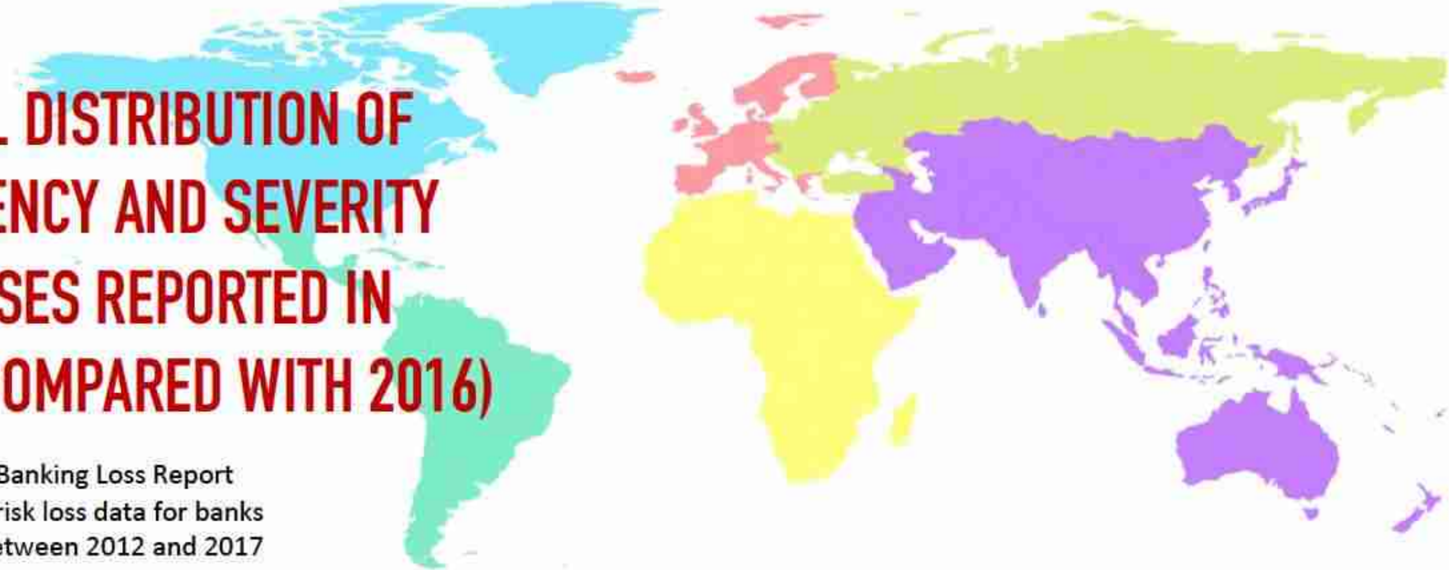
Western Europe

Frequency: 18,893 ▼ (20,750)
Total loss: €4.5Bn ▼ (€9.8bn)

Eastern Europe

Frequency: 1,613 ▲ (1,608)
Total loss: €0.4Bn – (€0.4bn)

GLOBAL DISTRIBUTION OF FREQUENCY AND SEVERITY OF LOSSES REPORTED IN 2017 (COMPARED WITH 2016)



REF: Annual Banking Loss Report
Operational risk loss data for banks
submitted between 2012 and 2017
June 2018

Latin America and the Caribbean

Frequency: 12,301 ▼ (13,630)
Total loss: €1.1Bn ▼ (€1.2bn)

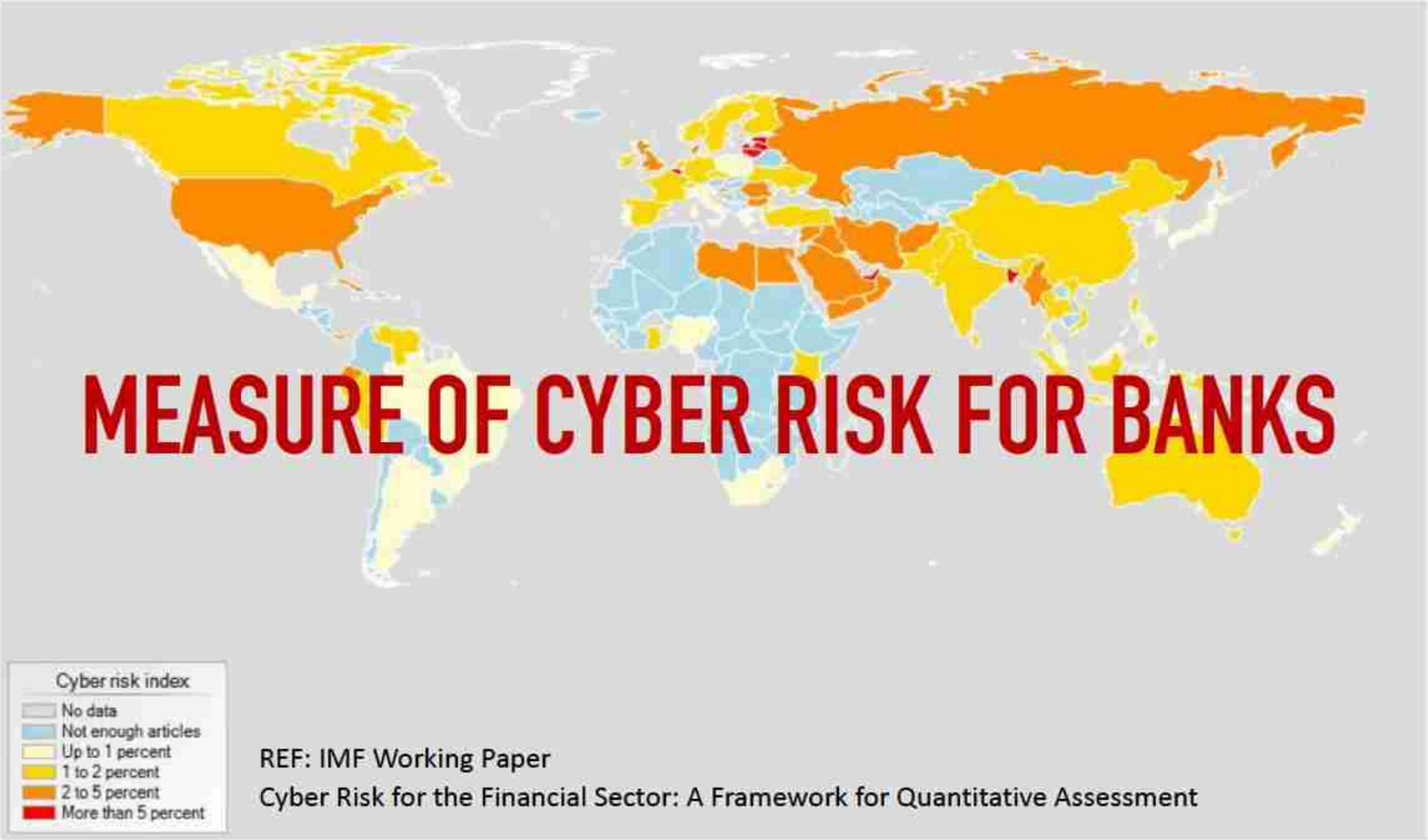
Africa

Frequency: 1,044 ▼ (1,185)
Total loss: €0.2Bn ▼ (€0.3bn)

Asia Pacific

Frequency: 2,962 ▼ (3,840)
Total loss: €1.5Bn ▲ (€1.3bn)

MEASURE OF CYBER RISK FOR BANKS



REF: IMF Working Paper

Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

Note: Number of articles featuring "cyber-attack" or "hack" or "cyber risk" or "cyber security" and "banks" or "bank" and "risk" divided by the number of articles featuring "banks" or "bank" and "risk" by country. The index is not computed for countries with fewer than 25 articles on cyber risk (light blue). Only articles in English were included. Period range: Jan-2014-Sep. 2017. Sources: Factiva; and author's calculations.

VULNERABILITIES IN FINANCIAL SECTORS

- Single Point of Failure and critical infrastructures
- Business disruptions in the financial sector
- Fraud
- Data breaches

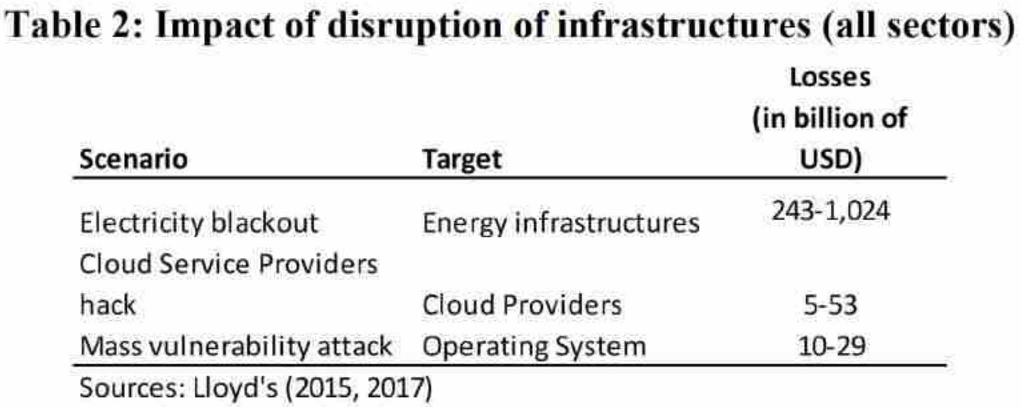


Table 2: Impact of disruption of infrastructures (all sectors)

Scenario	Target	Losses (in billion of USD)
Electricity blackout	Energy infrastructures	243-1,024
Cloud Service Providers hack	Cloud Providers	5-53
Mass vulnerability attack	Operating System	10-29

Sources: Lloyd's (2015, 2017)

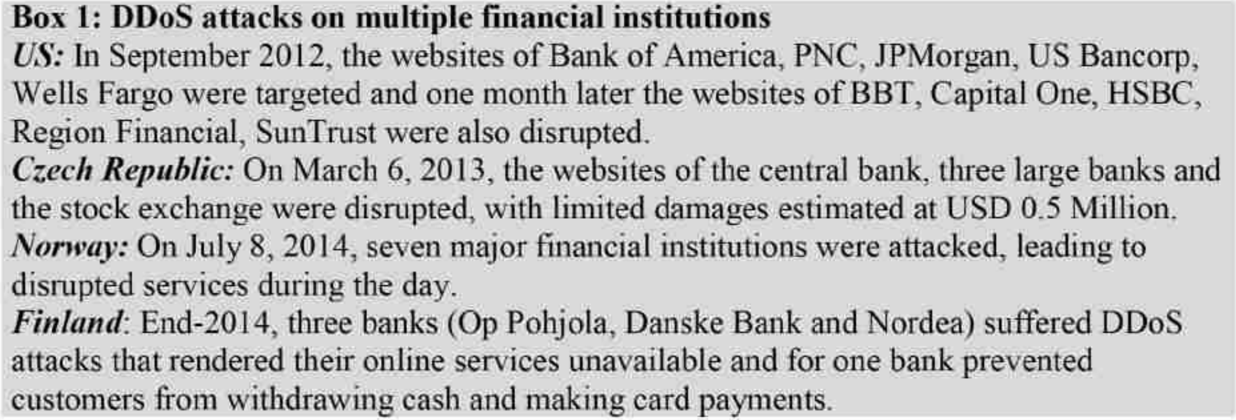
REF: IMF Working Paper

Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

R V CONNEX

VULNERABILITIES IN FINANCIAL SECTORS

- Single Point of Failure and critical infrastructures
- Business disruptions in the financial sector
- Fraud
- Data breaches



Box 1: DDoS attacks on multiple financial institutions

US: In September 2012, the websites of Bank of America, PNC, JPMorgan, US Bancorp, Wells Fargo were targeted and one month later the websites of BBT, Capital One, HSBC, Region Financial, SunTrust were also disrupted.

Czech Republic: On March 6, 2013, the websites of the central bank, three large banks and the stock exchange were disrupted, with limited damages estimated at USD 0.5 Million.

Norway: On July 8, 2014, seven major financial institutions were attacked, leading to disrupted services during the day.

Finland: End-2014, three banks (Op Pohjola, Danske Bank and Nordea) suffered DDoS attacks that rendered their online services unavailable and for one bank prevented customers from withdrawing cash and making card payments.

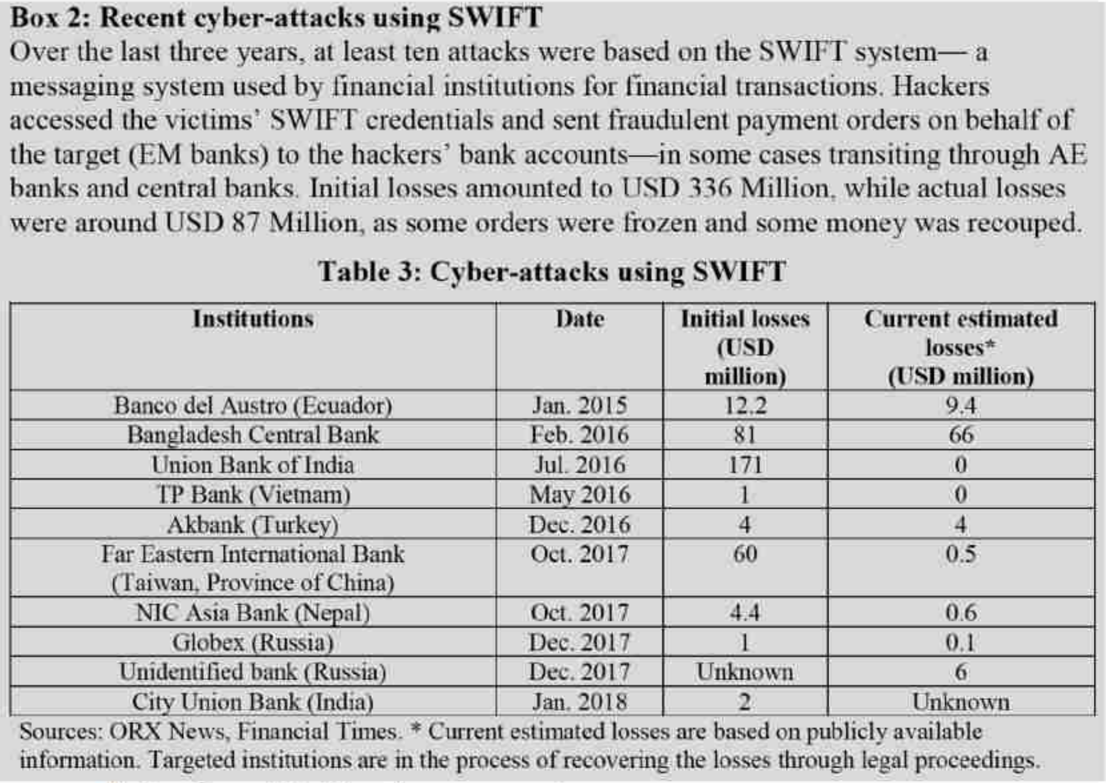
REF: IMF Working Paper

Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

R V CONNEX

VULNERABILITIES IN FINANCIAL SECTORS

- Single Point of Failure and critical infrastructures
- Business disruptions in the financial sector
- Fraud
- Data breaches



Box 2: Recent cyber-attacks using SWIFT

Over the last three years, at least ten attacks were based on the SWIFT system— a messaging system used by financial institutions for financial transactions. Hackers accessed the victims' SWIFT credentials and sent fraudulent payment orders on behalf of the target (EM banks) to the hackers' bank accounts—in some cases transiting through AE banks and central banks. Initial losses amounted to USD 336 Million, while actual losses were around USD 87 Million, as some orders were frozen and some money was recouped.

Table 3: Cyber-attacks using SWIFT

Institutions	Date	Initial losses (USD million)	Current estimated losses* (USD million)
Banco del Austro (Ecuador)	Jan. 2015	12.2	9.4
Bangladesh Central Bank	Feb. 2016	81	66
Union Bank of India	Jul. 2016	171	0
TP Bank (Vietnam)	May 2016	1	0
Akbank (Turkey)	Dec. 2016	4	4
Far Eastern International Bank (Taiwan, Province of China)	Oct. 2017	60	0.5
NIC Asia Bank (Nepal)	Oct. 2017	4.4	0.6
Globex (Russia)	Dec. 2017	1	0.1
Unidentified bank (Russia)	Dec. 2017	Unknown	6
City Union Bank (India)	Jan. 2018	2	Unknown

Sources: ORX News, Financial Times. * Current estimated losses are based on publicly available information. Targeted institutions are in the process of recovering the losses through legal proceedings.

REF: IMF Working Paper

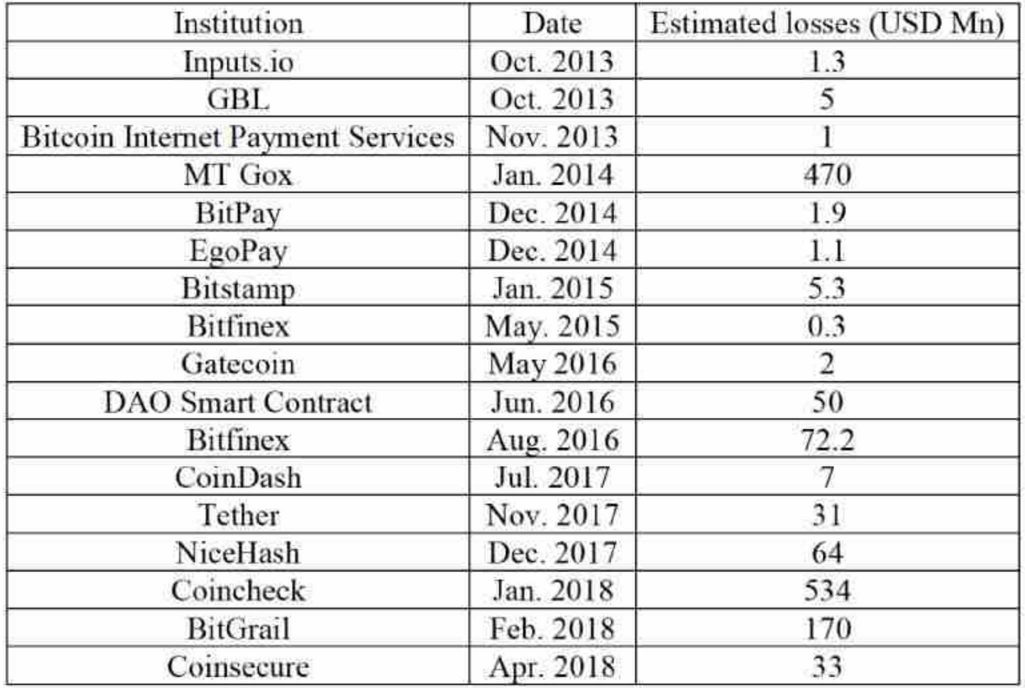
Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

R V CONNEX

VULNERABILITIES IN FINANCIAL SECTORS

- Single Point of Failure and critical infrastructures
- Business disruptions in the financial sector
- Fraud
- Data breaches

Table 4: Cyber-attacks on Fintech firms



Institution	Date	Estimated losses (USD Mn)
Inputs.io	Oct. 2013	1.3
GBL	Oct. 2013	5
Bitcoin Internet Payment Services	Nov. 2013	1
MT Gox	Jan. 2014	470
BitPay	Dec. 2014	1.9
EgoPay	Dec. 2014	1.1
Bitstamp	Jan. 2015	5.3
Bitfinex	May. 2015	0.3
Gatecoin	May 2016	2
DAO Smart Contract	Jun. 2016	50
Bitfinex	Aug. 2016	72.2
CoinDash	Jul. 2017	7
Tether	Nov. 2017	31
NiceHash	Dec. 2017	64
Coincheck	Jan. 2018	534
BitGrail	Feb. 2018	170
Coinsecure	Apr. 2018	33

Sources: ORX News, Financial Times

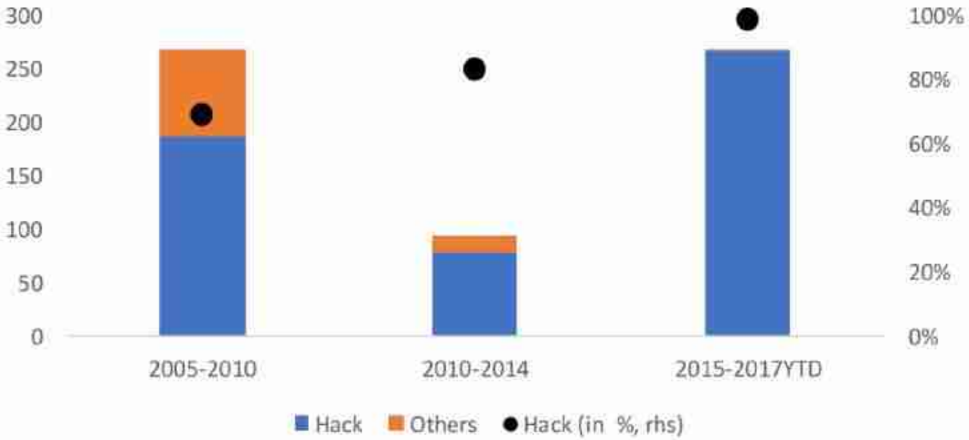
REF: IMF Working Paper

Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

VULNERABILITIES IN FINANCIAL SECTORS

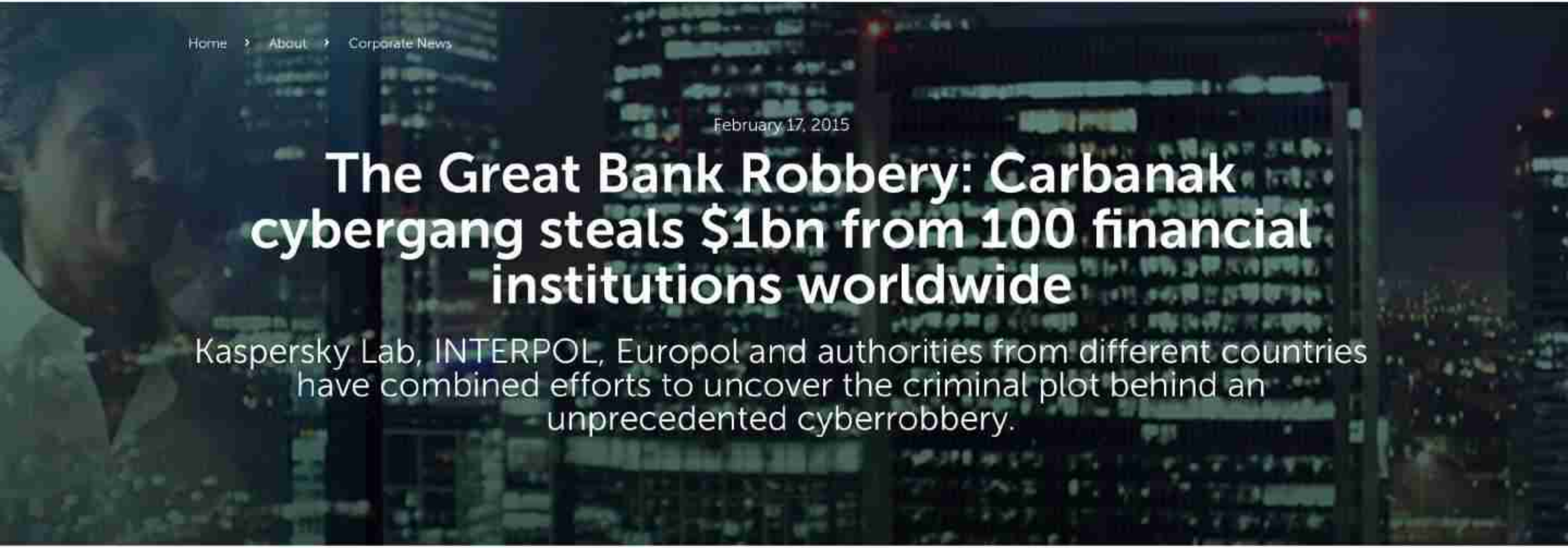
- Single Point of Failure and critical infrastructures
- Business disruptions in the financial sector
- Fraud
- Data breaches

Number of records breached in the financial sector in the U.S. (in million)



Source: Privacy Rights Clearinghouse

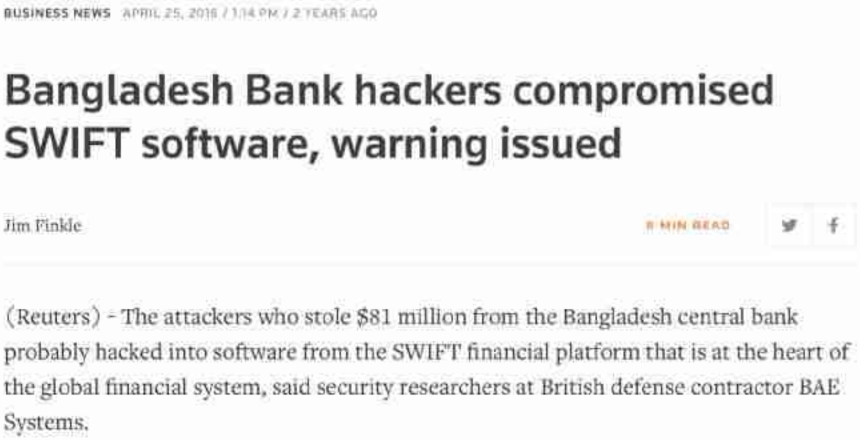
REF: IMF Working Paper
Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment



February 17, 2015

The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide

Kaspersky Lab, INTERPOL, Europol and authorities from different countries have combined efforts to uncover the criminal plot behind an unprecedented cyberrobbery.



BUSINESS NEWS APRIL 25, 2016 / 1:14 PM / 2 YEARS AGO

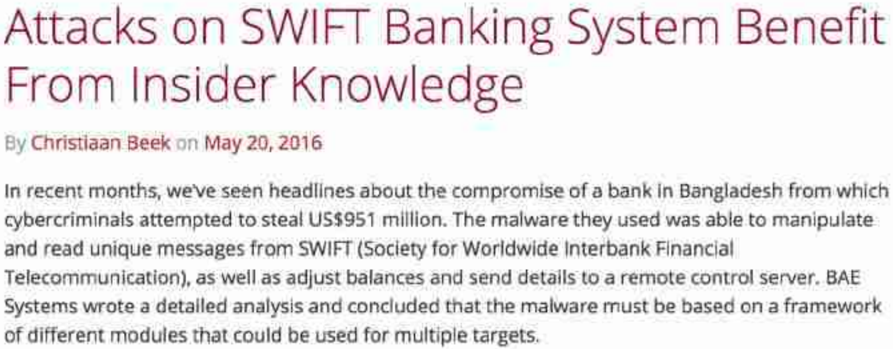
Bangladesh Bank hackers compromised SWIFT software, warning issued

Jim Finkle

8 MIN READ

(Reuters) - The attackers who stole $81 million from the Bangladesh central bank probably hacked into software from the SWIFT financial platform that is at the heart of the global financial system, said security researchers at British defense contractor BAE Systems.

REF: https://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv/bangladesh-bank-hackers-compromised-swift-software-warning-issued-idUSKCN0XM0DR

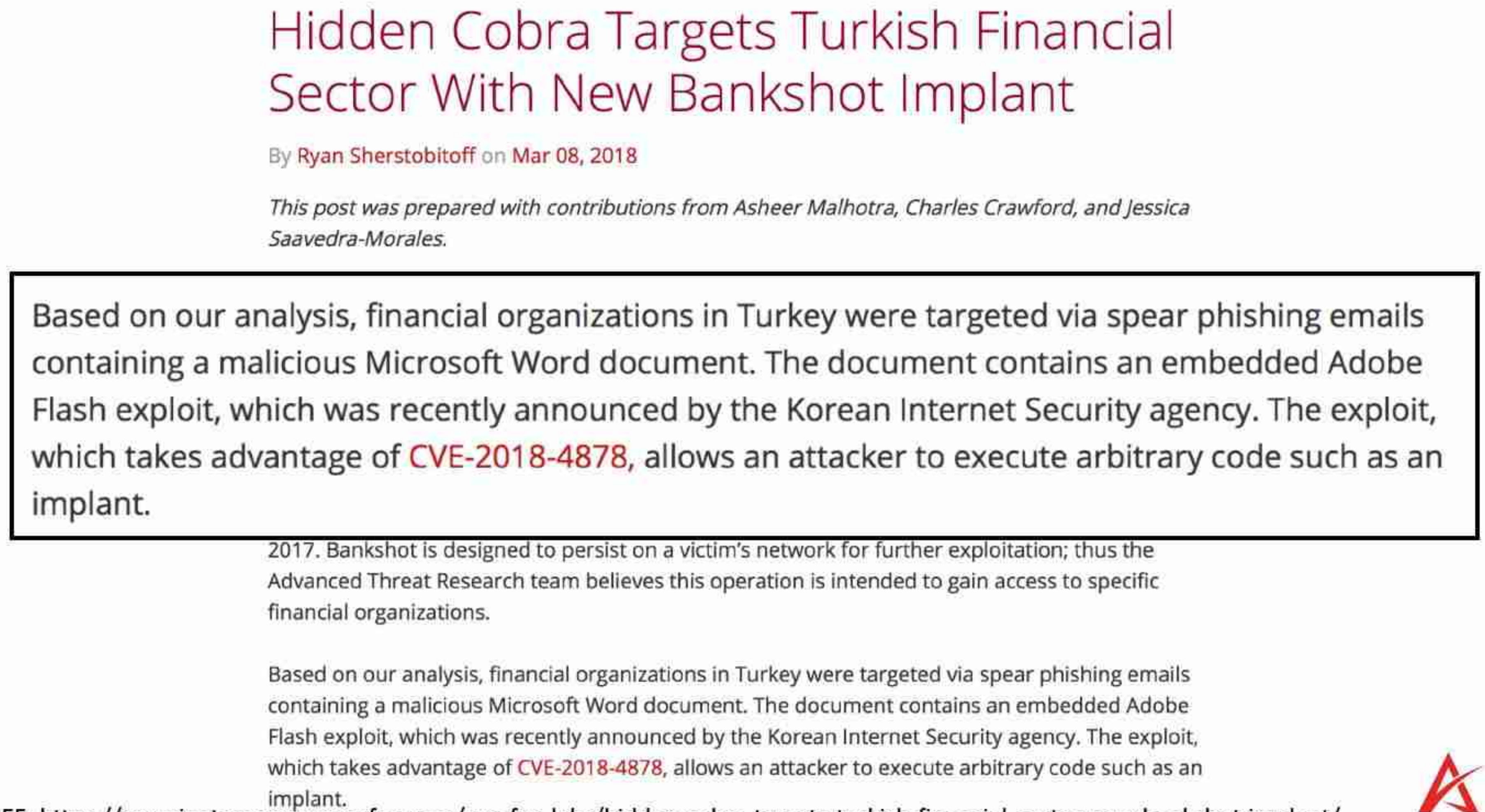


Attacks on SWIFT Banking System Benefit From Insider Knowledge

By Christiaan Beek on May 20, 2016

In recent months, we've seen headlines about the compromise of a bank in Bangladesh from which cybercriminals attempted to steal US$951 million. The malware they used was able to manipulate and read unique messages from SWIFT (Society for Worldwide Interbank Financial Telecommunication), as well as adjust balances and send details to a remote control server. BAE Systems wrote a detailed analysis and concluded that the malware must be based on a framework of different modules that could be used for multiple targets.

REF: https://securingtomorrow.mcafee.com/mcafee-labs/attacks-swift-banking-system-benefit-insider-knowledge/



Hidden Cobra Targets Turkish Financial Sector With New Bankshot Implant

By Ryan Sherstobitoff on Mar 08, 2018

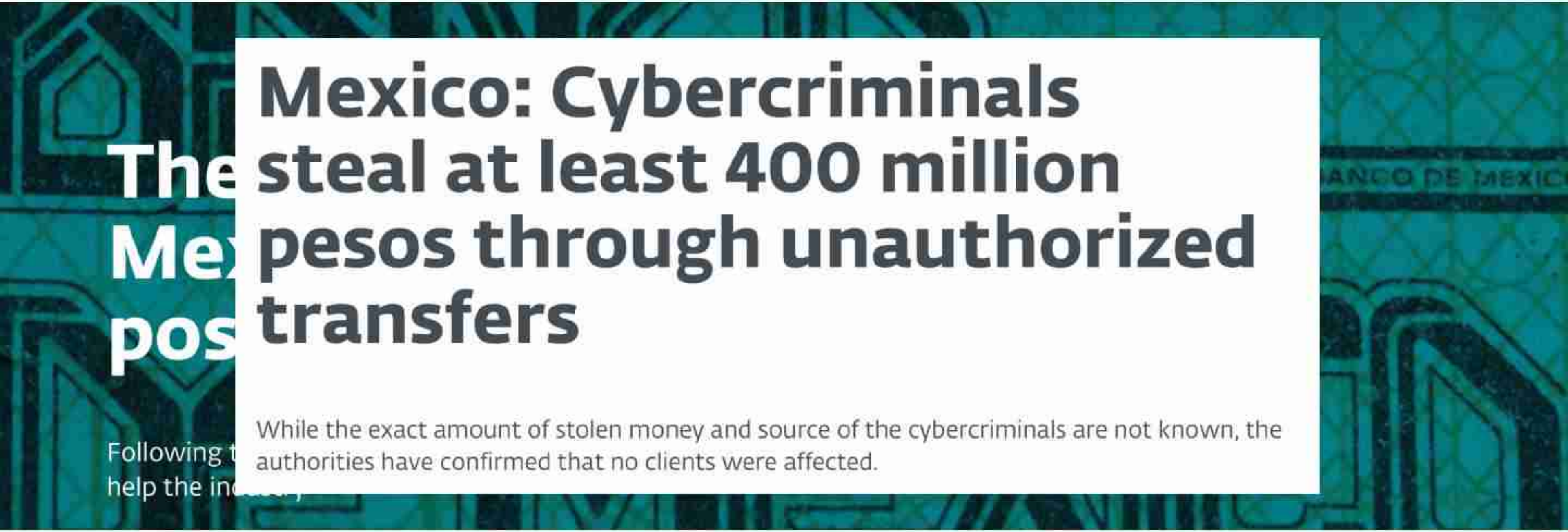
This post was prepared with contributions from Asheer Malhotra, Charles Crawford, and Jessica Saavedra-Morales.

Based on our analysis, financial organizations in Turkey were targeted via spear phishing emails containing a malicious Microsoft Word document. The document contains an embedded Adobe Flash exploit, which was recently announced by the Korean Internet Security agency. The exploit, which takes advantage of CVE-2018-4878, allows an attacker to execute arbitrary code such as an implant.

2017. Bankshot is designed to persist on a victim's network for further exploitation; thus the Advanced Threat Research team believes this operation is intended to gain access to specific financial organizations.

Based on our analysis, financial organizations in Turkey were targeted via spear phishing emails containing a malicious Microsoft Word document. The document contains an embedded Adobe Flash exploit, which was recently announced by the Korean Internet Security agency. The exploit, which takes advantage of CVE-2018-4878, allows an attacker to execute arbitrary code such as an implant.

REF: https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/



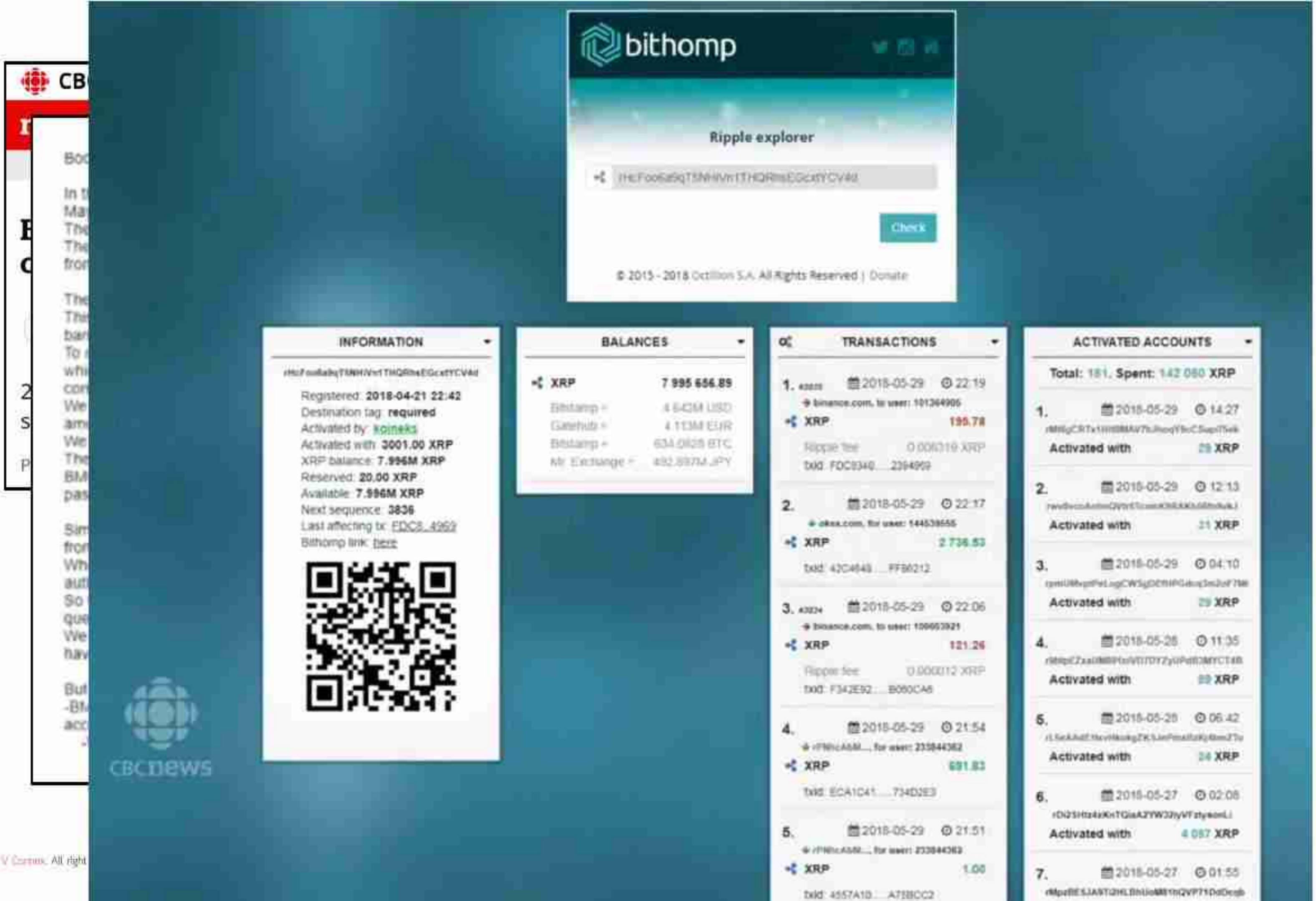
The
Me
pos

Following t
help the in

Mexico: Cybercriminals steal at least 400 million pesos through unauthorized transfers

While the exact amount of stolen money and source of the cybercriminals are not known, the authorities have confirmed that no clients were affected.

REF: https://www.welivesecurity.com/2018/06/05/cyberattack-on-banks-mexico-cybersecurity/



Ripple explorer

rHcFoo6a9qT5NHiVn1THQRhsEGcxtYCV4d

© 2015 - 2018 Octillion S.A. All Rights Reserved | Donate

INFORMATION

rHcFoo6a9qT5NHiVn1THQRhsEGcxtYCV4d

Registered: 2018-04-21 22:42
Destination tag: required
Activated by: koineks
Activated with: 3001.00 XRP
XRP balance: 7.996M XRP
Reserved: 20.00 XRP
Available: 7.996M XRP
Next sequence: 3836
Last affecting tx: FDC8...4969
Bithomp link: here

BALANCES

XRP	7 995 656.89
Bitstamp =	4.642M USD
Gatehub =	4.113M EUR
Bitstamp =	634.0826 BTC
Mr. Exchange =	492.897M JPY

TRANSACTIONS

1. 43835 2018-05-29 22:19
→ binance.com, to user: 101364906
XRP 195.78
Ripple fee 0.000019 XRP
txid: FDC8340.....2394969

2. 2018-05-29 22:17
← okex.com, for user: 144539555
XRP 2 736.53
txid: 42C4648.....FF86212

3. 43824 2018-05-29 22:06
→ binance.com, to user: 100653921
XRP 121.26
Ripple fee 0.000012 XRP
txid: F342E92.....B060CA6

4. 2018-05-29 21:54
← rPNhcA6M..., for user: 233844362
XRP 691.83
txid: ECA1C41.....734D2E3

5. 2018-05-29 21:51
← rPNhcA6M..., for user: 233844363
XRP 1.00
txid: 4557A10.....A73BCC2

ACTIVATED ACCOUNTS

Total: 181, Spent: 142 080 XRP

1. 2018-05-29 14:27
[illegible]
Activated with 29 XRP

2. 2018-05-29 12:13
[illegible]
Activated with 21 XRP

3. 2018-05-29 04:10
[illegible]
Activated with 29 XRP

4. 2018-05-28 11:35
[illegible]
Activated with 89 XRP

5. 2018-05-28 06:42
[illegible]
Activated with 24 XRP

6. 2018-05-27 02:08
[illegible]
Activated with 4 087 XRP

7. 2018-05-27 01:55
[illegible]

$800,000: XRP Phishing Scam Uncovered By South Korean Authorities, FBI

Omar Faridi

15 Sep 2018 / 471 views / In #Ripple , #Security , #Where's My Money?

- Scammers created a fake crypto trading website by replicating a real exchange site.
- Users were sent fraudulent emails with links to the fake XRP exchange, and their login details were stolen to access and steal their funds.

REF: https://www.cryptoglobe.com/latest/2018/09/800000-ripple-xrp-phishing-scam-uncovered-by-south-korean-authorities-fbi/

South Korean authorities and the US Federal Bureau of Investigation (FBI) have reportedly uncovered an $800,000 cryptocurrency phishing scam in which "dozens" of XRP investors had been targeted.

R V CONNEX

GDPR AND CYBERSECURITY

ALPHAWOLF R V CONNEX

DRIVER FOR DATA PRIVACY

Drivers

- Regulations
- Press Headlines
- Reputation
- Business Opportunity
- Customer Expectations

Inhibitors

- Lack of Business Ownership
- Data Growth
- Evolving Threat Landscape
- Lack of Visibility
- Emerging Technology

GENERAL DATA PROTECTION REGULATION (GDPR)

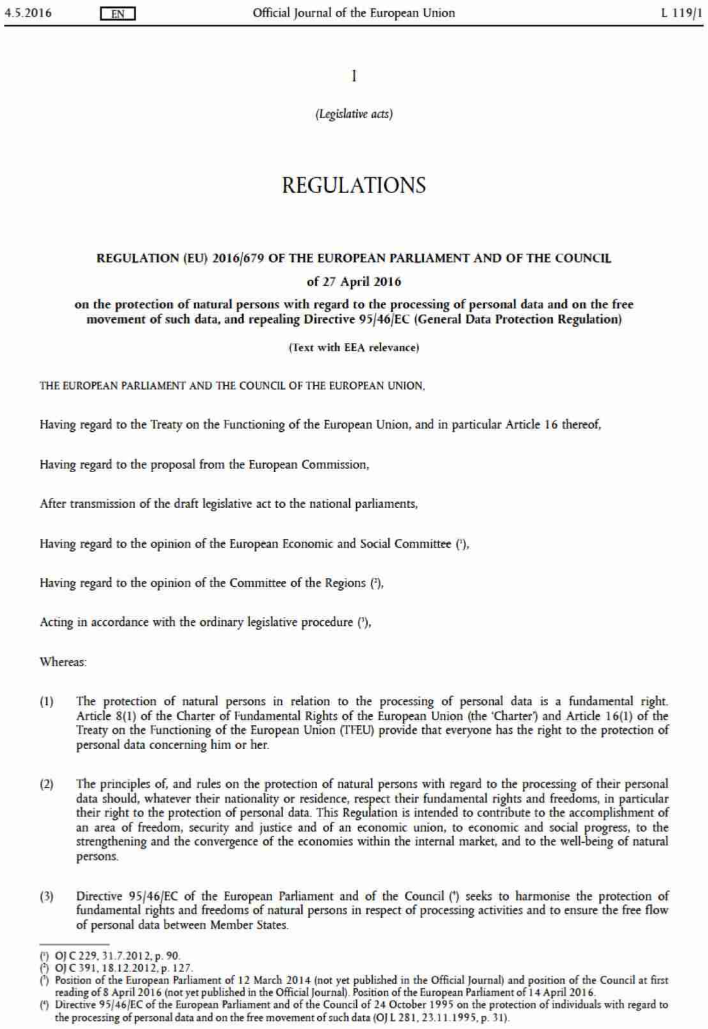
TODAY:

28 Interpretations of the Data Protection ***Directive***

2018:

One Data Protection ***Regulation*** Harmonized across all EU member states

- Right to be Forgotten
- Parental Consent
- Data Protection Officer
- Joint Liability of Controllers and Processors
- Extra-Territoriality of GDPR
- Fines and Penalties
- Mandatory Breach Notification



I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the Committee of the Regions [2],

Acting in accordance with the ordinary legislative procedure [3],

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council [4] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

[1] OJ C 229, 31.7.2012, p. 90.

[2] OJ C 391, 18.12.2012, p. 127.

[3] Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

ESSENTIAL GDPR FACTS

- The General Data Protection Regulation (GDPR) was approved by the EU Parliament on 14 April 2016. It will be enforceable on 25 May 2018.
- The GDPR replaces the Data Protection Directive 95/46/EC and was developed to harmonize data privacy laws across Europe and strengthen rights for individuals.
- As a regulation (not a directive), it will apply immediately in all EU territories. There is no need for countries to pass individual laws.
- The fines associated with breaching GDPR are considerable with the highest penalties resulting in fines of up to €20m or 4% of annual global turnover, whichever is greater.
- Data protection by design is a core principle for the GDPR. This means that data protection and privacy should be a priority in all organizations, not an afterthought.

25 May 2018—
GDPR is enforceable

Replaces outgoing Data
Protection Directive 95/46/EC

A regulation, not a directive

Fines up to €20m or
4% of global turnover

Data protection by design,
not by afterthought

GDPR CHAPTERS

1. General provisions
2. Principles
3. Rights of the data subject
4. Controller and processor
5. Transfers of personal data to third countries or international organisations
6. Independent supervisory authorities
7. Cooperation and consistency
8. Remedies, liability and penalties
9. Provisions relating to specific processing situations
10. Delegated acts and implementing acts
11. Final provisions

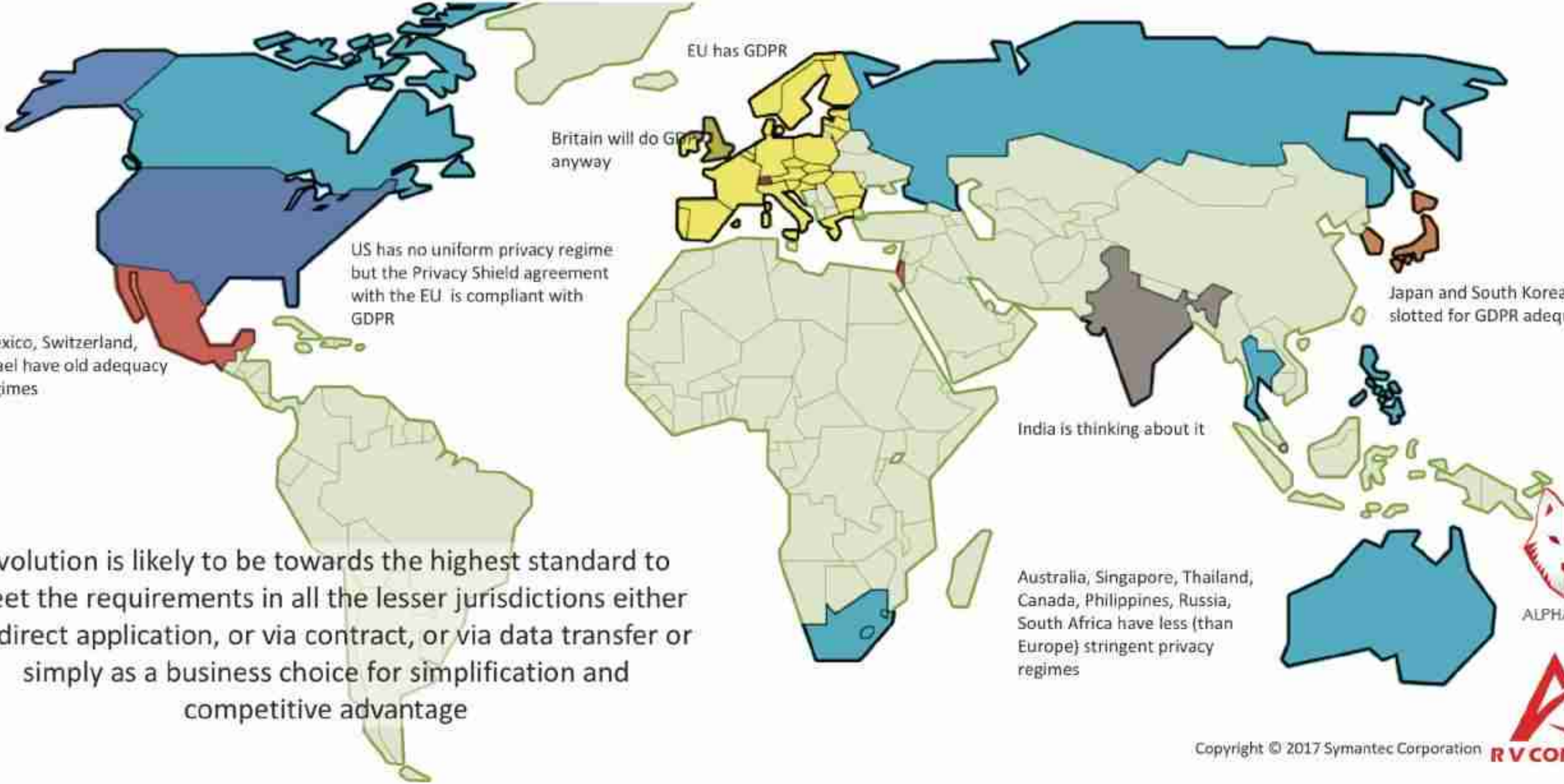
R V CONNEX

WHAT REGIONS ARE AFFECED BY GDPR?

Anywhere as long as you do business in Europe

Symantec.

IS THE WHOLE WORLD TURNING GDPR COMPLIANT?



EU has GDPR

Britain will do GDPR anyway

US has no uniform privacy regime but the Privacy Shield agreement with the EU is compliant with GDPR

Mexico, Switzerland, Israel have old adequacy regimes

Japan and South Korea are slotted for GDPR adequacy

India is thinking about it

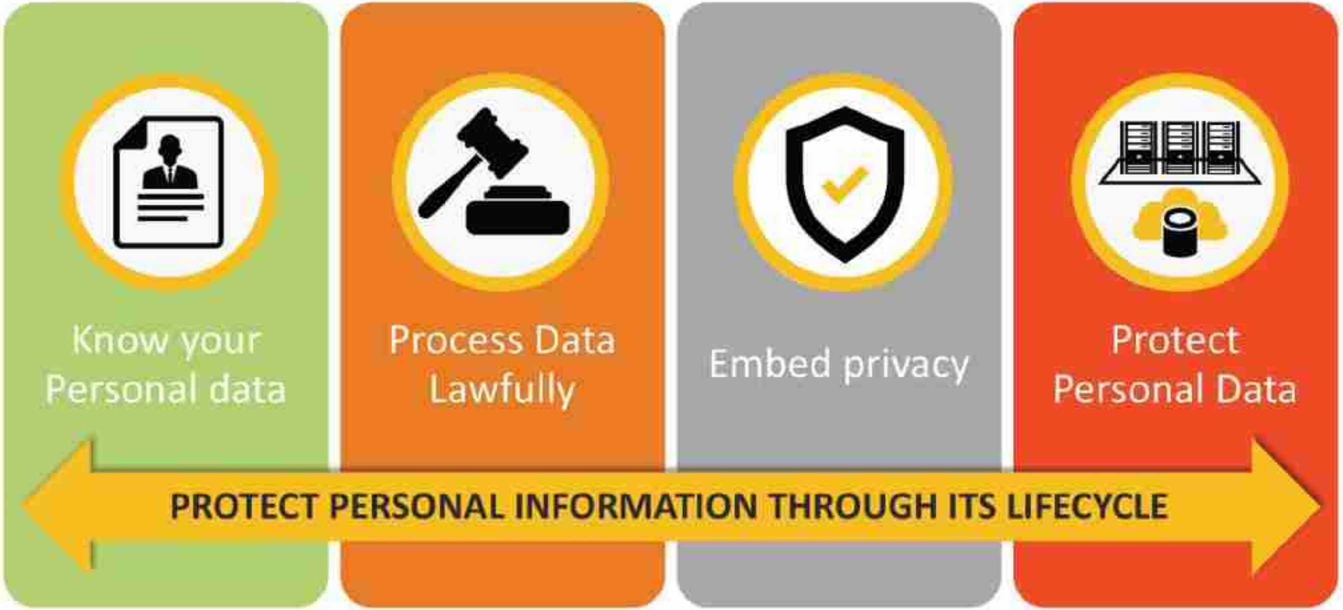
Australia, Singapore, Thailand, Canada, Philippines, Russia, South Africa have less (than Europe) stringent privacy regimes

Evolution is likely to be towards the highest standard to meet the requirements in all the lesser jurisdictions either by direct application, or via contract, or via data transfer or simply as a business choice for simplification and competitive advantage

ALPHAWOLF

R V CONNEX

GDPR TECHNOLOGY CONSIDERATION



Know your Personal data

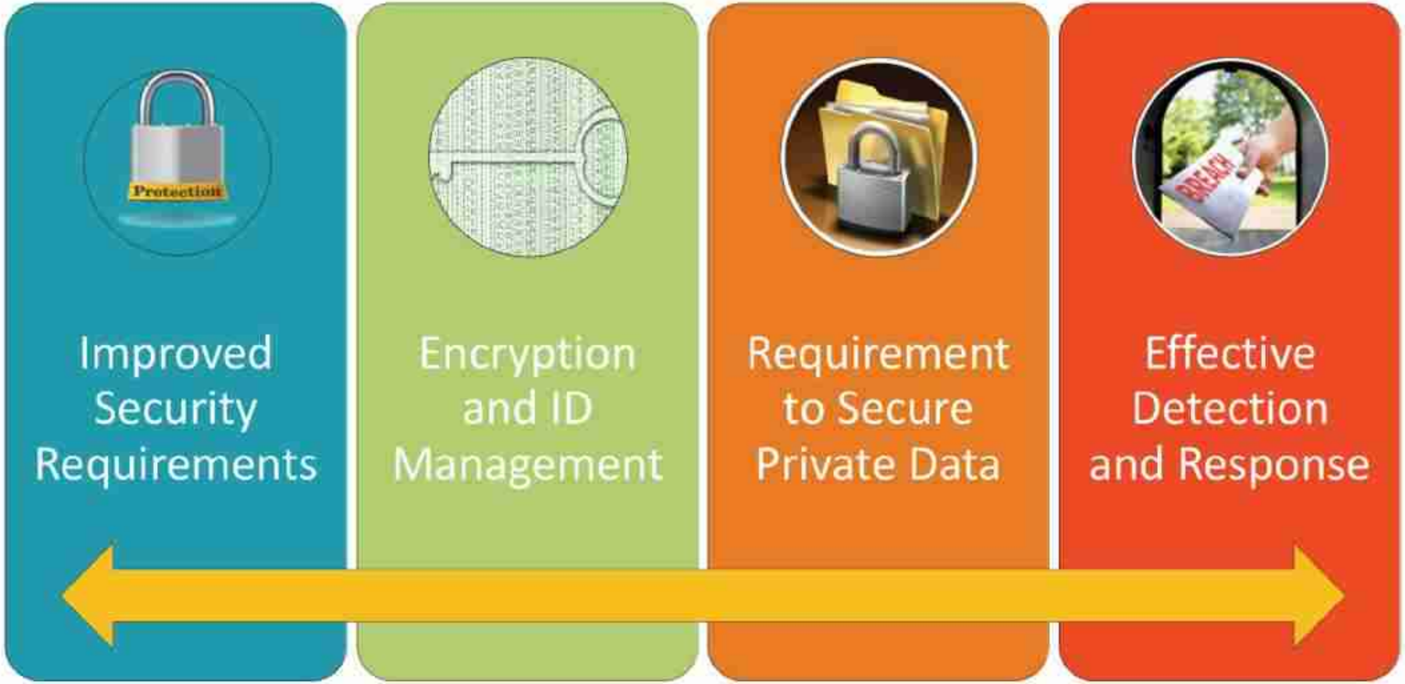
Process Data Lawfully

Embed privacy

Protect Personal Data

PROTECT PERSONAL INFORMATION THROUGH ITS LIFECYCLE

INFORMATION SECURITY



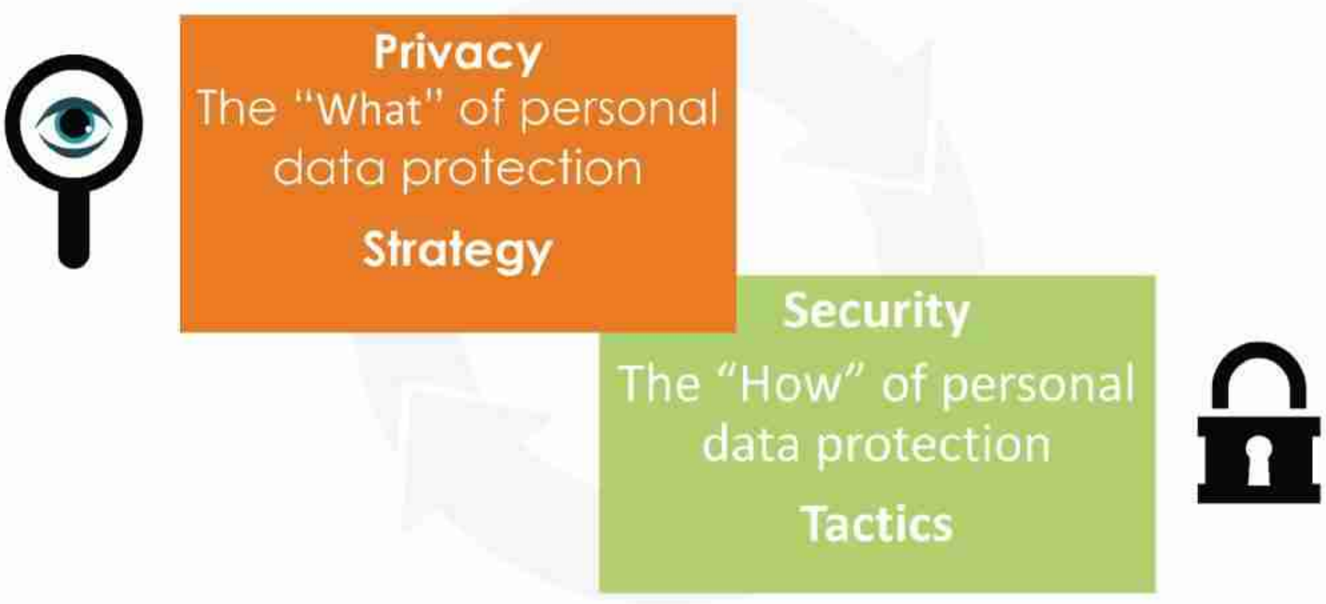
Improved Security Requirements

Encryption and ID Management

Requirement to Secure Private Data

Effective Detection and Response

PRIVACY & SECURITY



Privacy

The "What" of personal data protection

Strategy

Security

The "How" of personal data protection

Tactics

"You can have security without privacy but you can't have privacy without security"

Symantec.

KEY GDPR COMPLIANCE CONSIDERATIONS

And How Security Technical Controls Fit

Can you determine what your ***risk profile*** is?

What broad areas do I need to focus on for GDPR?

How do I manage and report on my information risk management practices?

What personal data is out there and ***where*** is it?

Can we ***control what*** personal data is accessible and ***who*** can access it?

Can we ***control where*** data resides?

Can we ***encrypt / obfuscate*** personal data?

Can we ***detect*** unauthorised access or breaches of personal data?

Can we quickly and thoroughly ***notify*** in the event of a breach?

Can we continuously evaluate the ***effectiveness*** of our security?

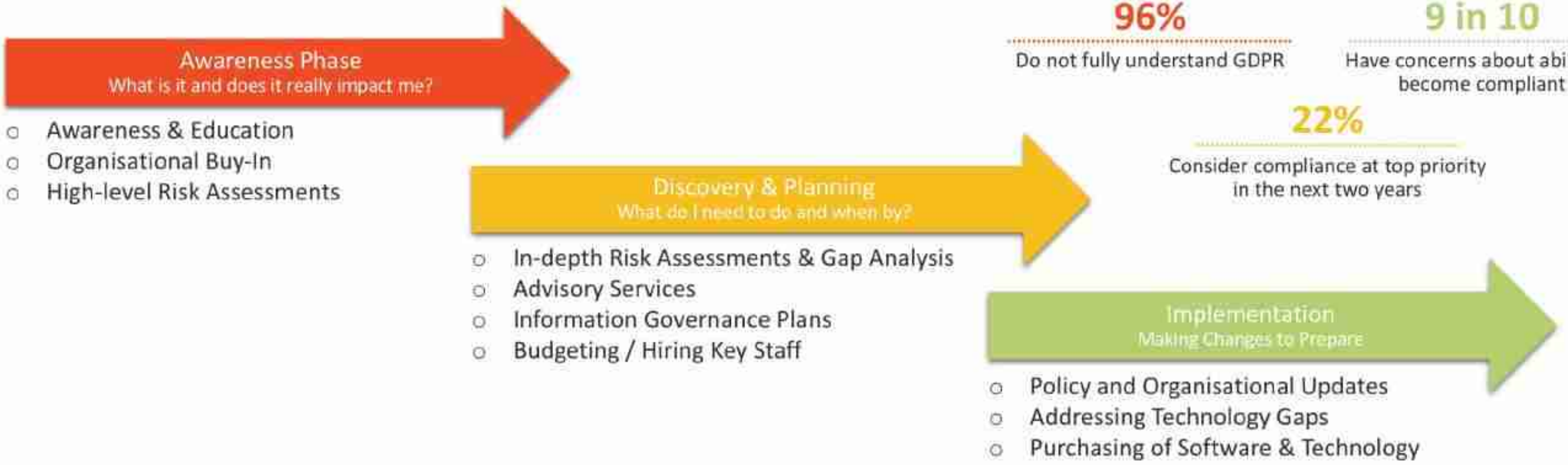
Risk Management
Compliance Assessments

Information Centric Security
DLP / CASB
Authentication
Encryption
Tokenisation

Breach Response
Managed Security and Incident Response Services
Security Analytics

TIMELINE FOR GDPR

Typical GDPR Use Cases Based on Maturity



Awareness Phase
What is it and does it really impact me?

- Awareness & Education
- Organisational Buy-In
- High-level Risk Assessments

Discovery & Planning
What do I need to do and when by?

- In-depth Risk Assessments & Gap Analysis
- Advisory Services
- Information Governance Plans
- Budgeting / Hiring Key Staff

Implementation
Making Changes to Prepare

- Policy and Organisational Updates
- Addressing Technology Gaps
- Purchasing of Software & Technology

96%
Do not fully understand GDPR

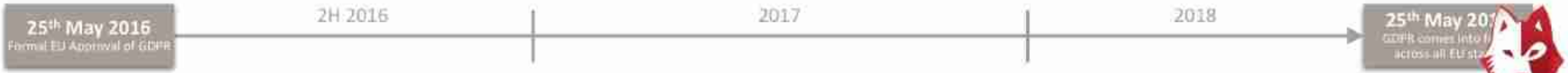
9 in 10
Have concerns about ability to become compliant

22%
Consider compliance at top priority in the next two years

USE CASE:
Mitigate Risk to Data Subjects

USE CASE:
Protect Against Personal Data Loss

USE CASE:
Minimise Risk in Case of a Breach



25th May 2016
Formal EU Approval of GDPR

2H 2016

2017

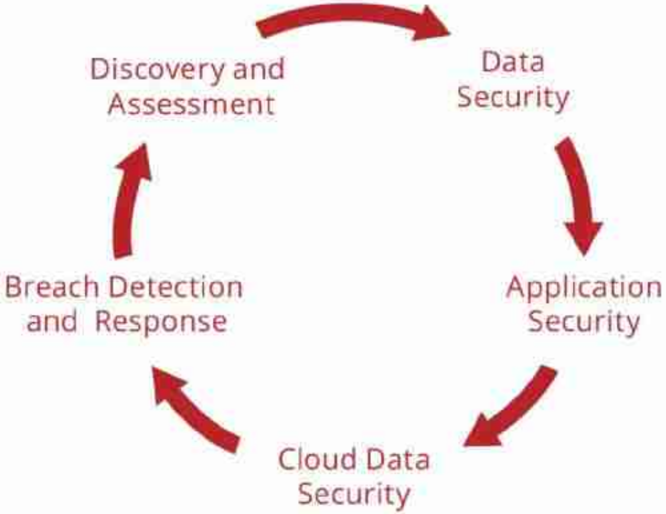
2018

25th May 201
GDPR comes into f
across all EU sta

DATA PROTECTION LIFECYCLE

McAfee Data Protection Lifecycle

Key Solution Areas for GDPR Readiness



Discovery and Assessment

Data Security

Application Security

Cloud Data Security

Breach Detection and Response

Step 1: Continuous Discovery and Assessment
Discover, classify, and inventory personal data.

Step 2: Data Security
Protect personal data at rest and in motion on endpoints and in the cloud.

Step 3: Application Security
Defend critical applications in the data center and cloud.

Step 4: Cloud Data Security
Safeguard personal data that is uploaded to the cloud, residing in the cloud, and downloaded from the cloud.

Step 5: Breach and Detection Response
Ensure that critical processes are in place to detect, investigate, and remediate breaches in a timely manner.

GDPR Articles	Requirements	Data Protection Lifecycle Phase
Article 5	Principles for processing data: • Transparent, fair, and lawful • Data collection for explicit and legitimate purposes • Accuracy of data • Data minimization • Limitations on storage of data • Security of personal data, including protection against unauthorized or unlawful use and against accidental loss, destruction, or damage	Discovery and assessment
Articles 25, 32	Data protection by design and security of processing: • Put measures in place to ensure that data is not accessible without the individual's intervention • Integrate data privacy into an information security policy • Encrypt personal data • Maintain security measures • Regularly test security posture	• Data protection • Application security • Cloud data protection
Article 30	Records of processing activity: • Inventory and classify data • Track how data is processed and for what purpose • Disclosure of entities with whom the data is shared or transferred	SOC breach detection
Article 33	Breach notification: • Notify an authority within 72 hours of becoming aware of a breach • Communicate the breach to the individuals affected by it	SOC breach detection

THE CAPABILITIES NEEDED TO BECOME GDPR READY

	Protection	Detection	Correction
Governance	■ Establish executive awareness and board-level support for cybersecurity and data protection ■ Appoint a data protection officer with appropriate authority to enforce compliance standards, to the extent that is necessary ■ Design a continuous compliance monitoring and assessment program for proactive compliance checks ■ Establish an information security management program based on industry-accepted frameworks (NIST, ISO27001, SABSA) and controls (SANS, etc.) ■ Foster a positive and collaborative culture of data security with the employees and business partners ■ Establish a security operations center and staff for 24/7 activity ■ Embed incident response and data protection language into cloud service provider and third-party supplier agreements		
People	■ Train and certify application developers on secure coding practices ■ Train and certify end users on data protection ■ Train and certify domain and technology administrators on secure configurations, responsibilities, and best practices ■ Train and certify domain and technology administrators on secure configurations	■ Train all users and administrators on data breach reporting procedures and responsibilities ■ Train and certify incident handlers on data breach reporting and handling requirements	■ Develop coaching mechanisms for positive reinforcement of data protection policies ■ Establish link between human resources and security for data protection policy violation handling ■ Establish a crisis action team to manage breach response actions
Processes	■ Establish a continuous application security testing process ■ Perform regular scans for databases and other sensitive data repositories ■ Embed data protection language into cloud provider and other third-party supplier agreements ■ Continuously review privileges and access rights to sensitive data repositories and applications ■ Develop a continuous data classification	■ Continuously monitor for data-at-rest encryption status across endpoints, data center, and cloud servers ■ Develop breach detection and response playbooks to identify accidental or malicious data loss scenarios ■ Continuously monitor for data breach scenarios ■ Develop reporting procedures to report data breaches to authorities within the required timeline ■ Embed incident detection language into cloud provider and other third-party supplier agreements	■ Exercise the crisis action team at least once per year ■ Develop response actions to isolate and fully understand the scope of a breach within four hours ■ Develop a continuously monitored vulnerability correction system for DevOps ■ Develop response action playbooks and rehearsals incorporating IT, SecOps, HR, PR, executive leadership, and business unit representatives
Technology	■ Advanced anti-malware solutions using signatures, intelligence, and behavioral analysis capability across end-user devices and servers ■ Encryption for data at rest on end-user devices, servers, and databases ■ Intrusion prevention systems for workload and application security ■ Network data loss prevention for data-in-motion security ■ Endpoint data loss prevention for data-in-use and in-motion security on end-user devices ■ Database Activity Monitoring to protect enterprise applications from exploit ■ Cloud Web Security Gateways for mobile data and threat prevention ■ Cloud Security Brokers to provide visibility and control of data in SaaS applications	■ Central visibility and policy management for data loss prevention and encryption tools ■ Security Information and Event Management system for real-time incident detection and forensics ■ Log collection system with capacity for at least six months but up to one-year storage for critical sensor and data sources ■ Secure evidence repository for data loss incident investigations ■ Endpoint detection and response tools with traffic and user activity history for incident triage ■ User behavior analytics to identify suspicious activity on enterprise and cloud applications	■ Automated policy-based encryption for data in motion on email, web, and cloud traffic ■ Response action tools capable of host, network, application, data, and user isolation to contain a breach

McAfee ALPHAWOLF R V CONNEX

MEASURING SECURITY OUTCOMES

	Protection	Detection	Correction
Neutralize Threats	- Prevent known or unknown malware installation on end-user devices, databases, and servers - Prevent application exploits that led to unauthorized access and data loss - Limit and control end-user and administrator privileges	- Identify, investigate, and validate malware infections wherever they occur - Identify, investigate, and validate exploit attempts on applications that host private data - Identify, investigate, and validate exploit attempts on databases that host private data	- Automatically share malware intelligence across sensors and control points - Isolate infected hosts or systems using pre-planned response and automated actions - Block malicious files on endpoints, network, and web channels using automated actions - Block command and control activity across network, web, or other channels using automated actions - Remove indicators of compromise from infected hosts or rebuild to prevent reinfection
Protect Data	- Use automated discovery and classification tools to identify and mark private data - Protect private data in use, at rest, or in motion from accidental or policy-based loss incidents - Protect private data in use, at rest, or in motion from malicious loss incidents - Prevent exfiltration of private data to known or unknown locations - Prevent unauthorized access to private data - Use automated encryption to identify and protect data in motion	- Identify, investigate, and validate policy-based data loss incidents - Identify, investigate, and validate malicious data exfiltration attempts - Identify, investigate, and validate exploit attempts on databases that host private data - Identify, investigate, and validate unauthorized access attempts to applications, databases, or servers that host private data	- Automatically share data intelligence across sensors and control points - Isolate infected hosts or systems using pre-planned response and automated actions - Isolate user privileges and access to private data using pre-planned response and automated actions - Use automated encryption to identify and correct potential data loss scenarios
Protect Cloud Environments	- Use automated discovery and classification tools to identify cloud applications and mark private data - Prevent known or unknown malware installation on cloud infrastructure-as-a-service servers - Prevent exploitation of cloud-hosted applications on infrastructure or platform - Protect private data in use, at rest, or in motion from accidental or malicious data loss incidents on cloud-hosted applications	- Identify, investigate, and validate unauthorized access to cloud-based services - Identify, investigate, and validate breaches of private data security controls on software-as-a-service applications - Identify, investigate, and validate breaches of private data security controls on hosted applications	- Automatically share data and malware intelligence across sensors and control points - Isolate infected hosts or systems using pre-planned response and automated actions - Isolate user privileges and access to private data using pre-planned response and automated actions - Use automated encryption to identify and correct potential data loss scenarios to cloud applications
Optimize Security Operations	- Continuously scan to identify and classify private data and data repositories - Continuously reduce attack surface for vulnerability and application exploits through patching and vulnerability scanning - Continuously monitor for protection control status across all managed end-user devices, databases, and servers	- Continuously monitor for indicators of compromise, particularly command and control activity - Continuously monitor for breaches of private data security controls - Continuously monitor for unauthorized access or privilege abuse attempts on systems with private data	- Use automation and integrated technologies to adapt security postures to prevent reinfection and private data exposure - Use automation and integrated technologies to quickly triage suspected infections, insider activity, or data loss indicators

McAfee

R V CONNEX

R V CONNEX

TRANSFORMING POTENTIAL

www.rvconnex.com

THANK YOU