# Cybersecurity and data privacy risks in the digital age

**Catherine Bromilow** 



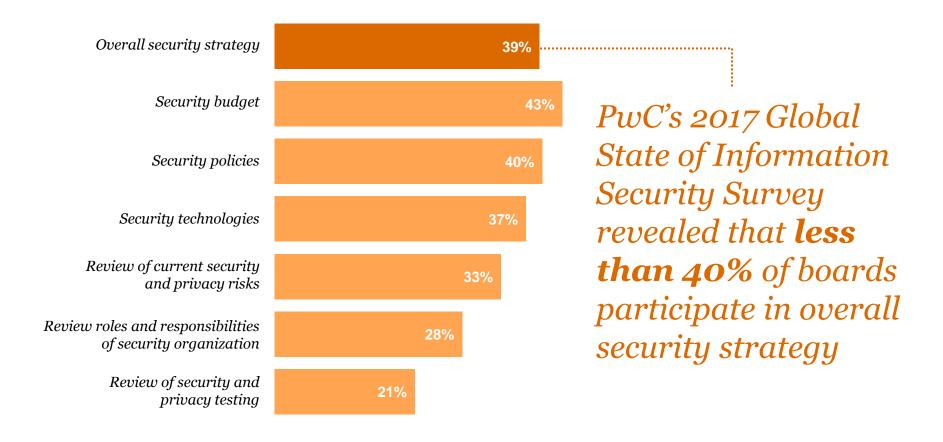




## The threat landscape

Adversary	Motives	Targets	Impact	
Nation State	• Economic, political, and/or military advantage	<ul> <li>Trade secrets</li> <li>Sensitive business information</li> <li>Emerging technologies</li> <li>Critical infrastructure</li> </ul>	<ul> <li>Loss of competitive advantage</li> <li>Disruption to critical infrastructure</li> </ul>	
Terrorists	<ul> <li>Immediate financial gain</li> <li>Influence political and / or social change</li> <li>Identify and attract supporters</li> </ul>	<ul><li> Critical Infrastructure</li><li> Anything of value</li><li> Ideological supporters</li></ul>	<ul> <li>Disruption to critical infrastructure</li> <li>Policy / social change</li> <li>New supporters</li> </ul>	
Organized Crime and Criminals	<ul><li>Immediate financial gain</li><li>Collect information for future financial gains</li></ul>	<ul> <li>Financial / Payment Systems</li> <li>Personally Identifiable Information</li> <li>Payment Card Information</li> <li>Protected Health Information</li> </ul>	<ul> <li>Costly regulatory inquiries and penalties</li> <li>Consumer and shareholder lawsuits</li> <li>Loss of consumer confidence</li> </ul>	
Hacktivists	<ul> <li>Influence political and /or social change</li> <li>Pressure business to change their practices</li> </ul>	<ul> <li>Corporate secrets</li> <li>Sensitive business information</li> <li>Information related to key executives, employees, customers &amp; business partners</li> </ul>	<ul><li>Disruption of business activities</li><li>Brand and reputation</li><li>Loss of consumer confidence</li></ul>	
• Insiders	<ul> <li>Personal advantage, monetary gain</li> <li>Professional revenge</li> <li>Patriotism</li> </ul>	<ul><li>Sales, deals, market strategies</li><li>Corporate secrets, IP, R&amp;D</li><li>Business operations</li><li>Personnel information</li></ul>	<ul> <li>Trade secret disclosure</li> <li>Operational disruption</li> <li>Brand and reputation</li> <li>National security impact</li> </ul>	

### Security areas in which boards actively participate



Q: In which of the following areas does your organization's Board of Directors actively participate? Source: PwC, 2017 Global State of Information Security Survey, 2017.

## Cybersecurity Dashboard considerations

#### Key Performance Indicators (KPI)\*

#### Operational activity Security related projects Information security Governance training **Business continuity** Crisis Management Risk management Internal audit External audit Compliance • Legal compliance Regulatory compliance

#### **Dashboard Samples**

Recent Actions

#### **Board Oversight Duties**

Overall Posture

•						
				_		_
Cyber Threat Trends  Control Effectiveness			R1	R2	R3	Status
Data A		Transfer Monitoring	Х		Х	7
	Payment Anomaly Detection		Х			<b>→</b>
Card Fraud Profiling				Х	<b>→</b>	
	Coverage of Data	a Leakage Protection	Х			<b>→</b>
	Security Operation	on		Х		7
			Х		X	<b>→</b>
	•	Payment Anomal Card Fraud Profil Coverage of Data Security Operation	Data Access and Transfer Monitoring  Payment Anomaly Detection	Data Access and Transfer Monitoring X  Payment Anomaly Detection X  Card Fraud Profiling  Coverage of Data Leakage Protection X  Security Operation  Supplier Management X	Data Access and Transfer Monitoring X  Payment Anomaly Detection X  Card Fraud Profiling  Coverage of Data Leakage Protection X  Security Operation X  Supplier Management X	Data Access and Transfer Monitoring X X  Payment Anomaly Detection X  Card Fraud Profiling X  Coverage of Data Leakage Protection X  Security Operation X  Supplier Management X X

Advanced Baseline Foundational

Rudimentary

<sup>\*</sup>Source: Information Security Forum Briefing No. 7, February 2008

## Questions management and boards should be asking

- Do security best practices dictate that the chief information security
  officer report directly to the board on a periodic basis regarding
  cybersecurity/privacy protection and practices?
- Is **outsourcing** data storage a better security system than at least most companies can securely do on their own?
- Regarding "cyber insurance," what does it truly cover? Will an insurer refuse to cover you if they say you didn't meet certain standards, duties and obligations?
- When does one bring an external "auditor" into the investigation?
- Do companies **share breach experience/solutions** with competitors so everyone learns or is this competitiveness barrier?
- Where a **merger or acquisition** is contemplated, is a review of the sufficiency and integrity of cyber protections necessary?
- What does a board "dashboard" look like regarding cybersecurity?





Privacy operations must keep pace with increasingly complex regulations and expanded commercial uses of data

**The past:**Run the business

**The present:** *Grow the business* 

The future:
Transform the business

#### Minimal regulatory oversight:

- Safe Harbor allows self-certification
- 10 countries with data protection (1998)
- EU Data Directive introduced (1995)
- Limited data use and collection of Personally Identifiable Information (PII)
- · Analytics use is minimal

#### Emerging laws and heavy fines:

- Safe Harbor invalidated, 4,700 US companies left in flux
- EU GDPR passed, implementation phase begins (2016)
- Fines out of the EU increase dramatically
- 100 countries with data protection regulations (2013)
- Product personalization gains in popularity

#### **Business disruptor:**

- GDPR in effect (potential for fines up to 4% annual turnover)
- Regulations like data localization require businesses to physically host data
- GDPR capabilities adopted more globally (e.g., Mexico, Brazil)
- 150 countries with data protection regulations (est. 2020)
- PII use drives new products and service offerings
- PII used by analytics across all areas of business
- Different types of PII generated, e.g., Internet of Things

1995 – 2005 2005 – 2018 2018 and beyond

## What is the General Data Protection Regulation (GDPR)?

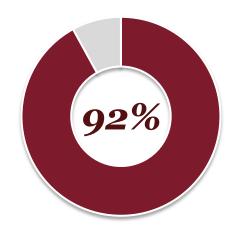
The GDPR is a new law in the European Union (EU) providing for uniform data protection regulation throughout the EU. When it goes into effect on May 25, 2018, it will represent one of the highest standards of data protection in the world, creating a consistent, global, and unified legal basis for data protection and enforcement across the Member-States. It will supersede the existing EU Data Protection Directive, which came into effect almost 20 years ago in 1998.

#### **Key GDPR requirements**

Multinationals doing business in Europe are seeing five GDPR requirements in particular cause the biggest impact on their future business plans:

- Mandatory data inventorying and record keeping of all internal and third-party processing of European personal data;
- **Mandatory data-breach notification** to regulators and individuals whose information is compromised following information-security failures;
- **Comprehensive individual rights** to access, correct, port, erase, and object to the processing of their data;
- Routine data-protection impact assessments for technology and business change; and
- Mandatory data protection officers and an overall rethinking of privacy strategy, governance, and risk management.





of survey respondents say GDPR compliance is a top data protection priority

#### Key questions

- What is the company's digital strategy and how does management assess its effectiveness? How will data be used to create value?
- Does the company have a process to consider the impact of privacy on new products or services?
- How does management identify, measure and manage its data privacy risk?
- What is management's strategy to achieve compliance with the General Data Protection Regulation? Is the remediation plan risk based? Will the company be able to provide evidence of compliance to privacy regulators?
- Does the company understand its global privacy compliance requirements? How will emerging privacy standards impact management's strategy?

## Thank you



© 2017 PwC. All rights reserved.

PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.