

Cybersecurity and data privacy risks in the digital age

Catherine Bromilow

October 3, 2017










Cybersecurity

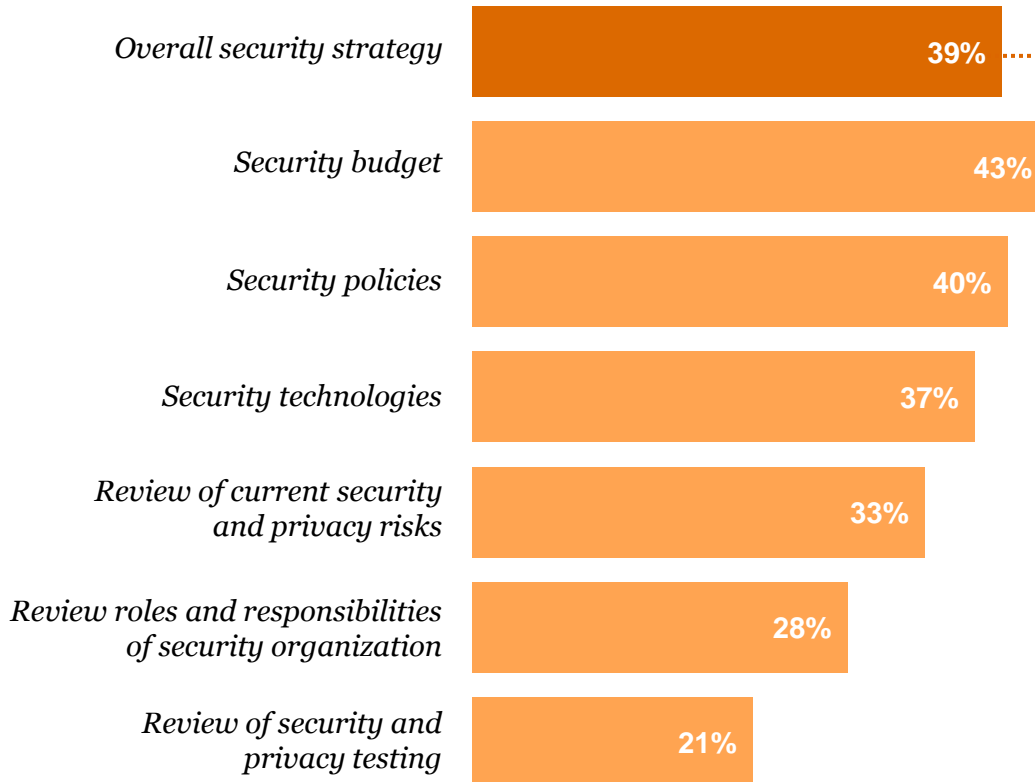
Cybersecurity

The threat landscape

Adversary	Motives	Targets	Impact
 Nation State	<ul style="list-style-type: none"> • Economic, political, and/or military advantage 	<ul style="list-style-type: none"> • Trade secrets • Sensitive business information • Emerging technologies • Critical infrastructure 	<ul style="list-style-type: none"> • Loss of competitive advantage • Disruption to critical infrastructure
 Terrorists	<ul style="list-style-type: none"> • Immediate financial gain • Influence political and / or social change • Identify and attract supporters 	<ul style="list-style-type: none"> • Critical Infrastructure • Anything of value • Ideological supporters 	<ul style="list-style-type: none"> • Disruption to critical infrastructure • Policy / social change • New supporters
 Organized Crime and Criminals	<ul style="list-style-type: none"> • Immediate financial gain • Collect information for future financial gains 	<ul style="list-style-type: none"> • Financial / Payment Systems • Personally Identifiable Information • Payment Card Information • Protected Health Information 	<ul style="list-style-type: none"> • Costly regulatory inquiries and penalties • Consumer and shareholder lawsuits • Loss of consumer confidence
 Hacktivists	<ul style="list-style-type: none"> • Influence political and /or social change • Pressure business to change their practices 	<ul style="list-style-type: none"> • Corporate secrets • Sensitive business information • Information related to key executives, employees, customers & business partners 	<ul style="list-style-type: none"> • Disruption of business activities • Brand and reputation • Loss of consumer confidence
 Insiders	<ul style="list-style-type: none"> • Personal advantage, monetary gain • Professional revenge • Patriotism 	<ul style="list-style-type: none"> • Sales, deals, market strategies • Corporate secrets, IP, R&D • Business operations • Personnel information 	<ul style="list-style-type: none"> • Trade secret disclosure • Operational disruption • Brand and reputation • National security impact

Cybersecurity

Security areas in which boards actively participate



*PwC's 2017 Global State of Information Security Survey revealed that **less than 40%** of boards participate in overall security strategy*

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)*



Dashboard Samples

Board Oversight Duties

Overall Posture



Board Duty	Status	Recent Actions	Areas of Note
Regulatory Compliance	●		
At-Risk Assets	●		
Mitigation Activities	●		
Cyber Threat Trends	●		

Control Effectiveness

	R1	R2	R3	Status
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	→

Cutting Edge
 Advanced
 Baseline
 Foundational
 Rudimentary

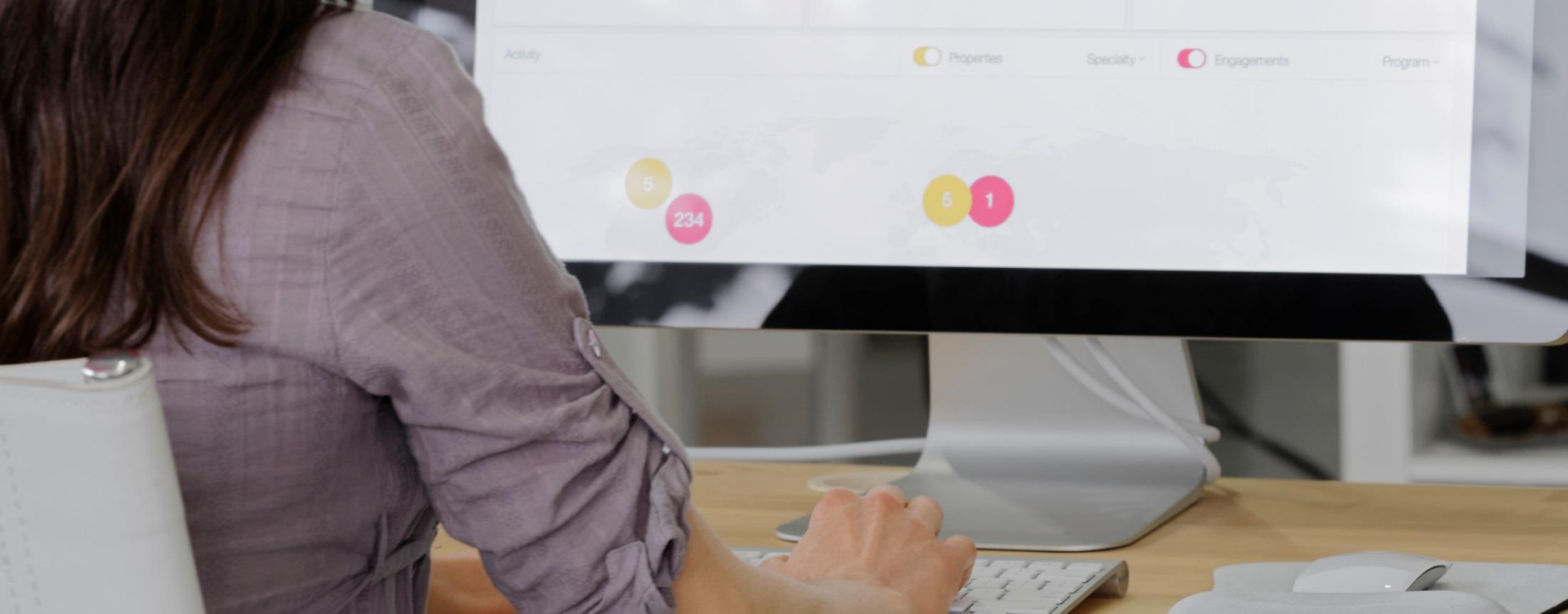
*Source: Information Security Forum Briefing No. 7, February 2008

Cybersecurity

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?

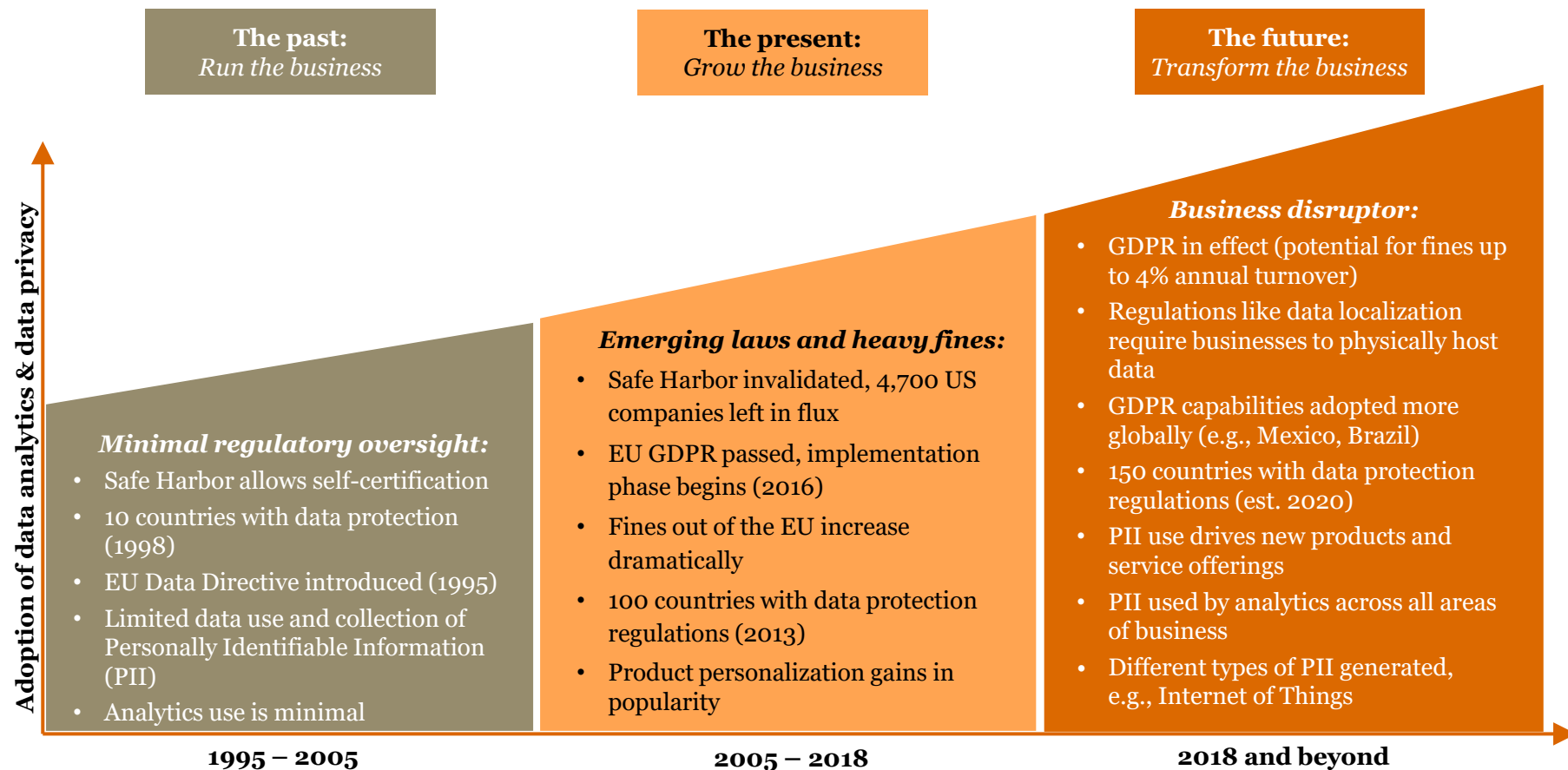




Data privacy

Data privacy

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



Data privacy

What is the General Data Protection Regulation (GDPR)?

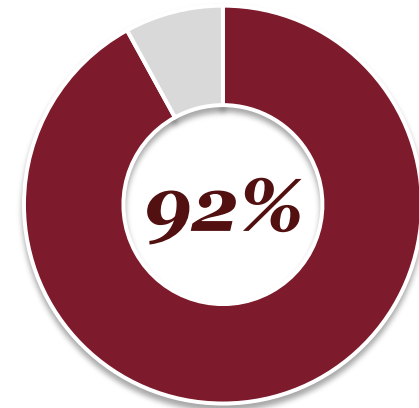
*The GDPR is a new law in the European Union (EU) providing for **uniform data protection regulation throughout the EU**. When it goes into effect on May 25, 2018, it will represent **one of the highest standards of data protection in the world**, creating a **consistent, global, and unified legal basis** 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.

Source: PwC, *GDPR preparedness pulse survey of US multinationals*, December 2016.



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

Data privacy

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

