FORRESTER®

For: CIOs

CIOs: Drive Internet-Of-Things Strategies Forward With Effective Data Protection Practices

by Enza Iannopollo, May 13, 2015

KEY TAKEAWAYS

The Internet Of Things Makes Firms' Technology, Systems, And Processes Visible

Thanks to the Internet of Things, connectivity is becoming the virtual connecting tissue between business processes. It also connects the firm with what's outside, exposing technology, systems, and processes as the line between "internal" and "external" blurs. Your BT's excellence (or failure) has never had a greater impact on the business.

Data Protection's Impact Goes Beyond Compliance

With the Internet of Things, an unprecedented amount of customers' intimate data hits firms' platforms. This should worry every firm, particularly given growing fines for noncompliance. But only a few have realized that the cost of damage to their business reputation and to their relationship with their customers is even greater.

CIOs: Drive Internet-Of-Things Strategies Forward With Effective Data Protection Practices

by Enza Iannopollo
with Pascal Matzke, Frank E. Gillett, Heidi Shey, and Carmen Stoica

WHY READ THIS REPORT

The Internet of Things (IoT) is disrupting every business, whether it's through the latest connected wearable devices or sensors digitizing traditional processes. As a result, firms must learn to interact with their customers in a whole new way: Winning, serving, and retaining customers has never being easier. However, success hinges on firms' ability to meet and exceed customers' expectations for data protection. What's at stake in the context of the Internet of Things is not only your corporate duty to mitigate compliance risks but also your ability to generate a sense of trust among your customers in order to take engagement to the next level. This report helps CIOs assess the impact of data protection rules on the life cycle of their B2B and B2C customers. It also provides CIOs with a guide and a checklist to evaluate the effectiveness of their firms' data protection practices while driving IoT initiatives to success.

Table Of Contents

Notes & Resources

Forrester interviewed seven vendor and user companies, including DLA Piper, ePrivacy, FireEye, Symantec, T-Systems, Telefónica, and Tune.

Related Research Documents

Brief: CIOs Will Architect And Operate The Internet Of Things

Customer Privacy Is A European CIO Priority

Mitigate Risks In The Customer's Journey

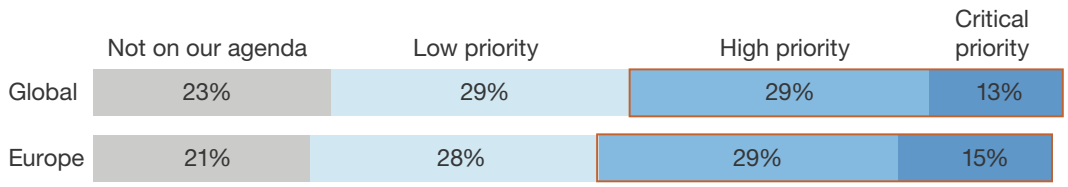
THE INTERNET OF THINGS: A BOOMING PLATFORM FOR CUSTOMER ENGAGEMENT

The Internet of Things (IoT) is a disruptive force. It is radically changing the way that firms deliver products and services to customers and how they work with partner ecosystems. It offers the potential for much deeper customer engagement than ever before. The market opportunity is huge, with government and utility/telecoms topping the list of the ripest sectors.[1] After their initial focus on the Internet of Things' benefits in terms of efficiency and cost savings, CIOs are now implementing IoT platforms to enable the creation of new business value.[2] It's hardly surprising, therefore, that 45% of European and 42% of global technology and business decision-makers consider it to be a top strategic priority (see Figure 1).[3]

Figure 1 The Internet Of Things Is A Top Strategic Priority

"Which of the following initiatives are likely to be your company's/group's top strategic network and telecommunications priorities during the next 12 months?"

Expand machine-to-machine (M2M) or "Internet of Things" initiatives



Base: 3,140 global and 892 European technology and business decision-makers

Note: Responses of "Don't know" are excluded.
Source: Forrester's Business Technographics® Global Networks And Telecommunications Survey, 2014

Poor Data Protection Practices Compromise The Success Of IoT Initiatives . . .

IoT platforms allow firms to know their customers and business partners in much greater detail, enabling firms to build more intimate, trustworthy, and direct relationships with them. But leveraging data, including personal data, to build that engagement means that the CIO, in conjunction with the chief information security officer (CISO) and chief privacy officer (CPO), must go the extra mile to protect customers' data.[4]

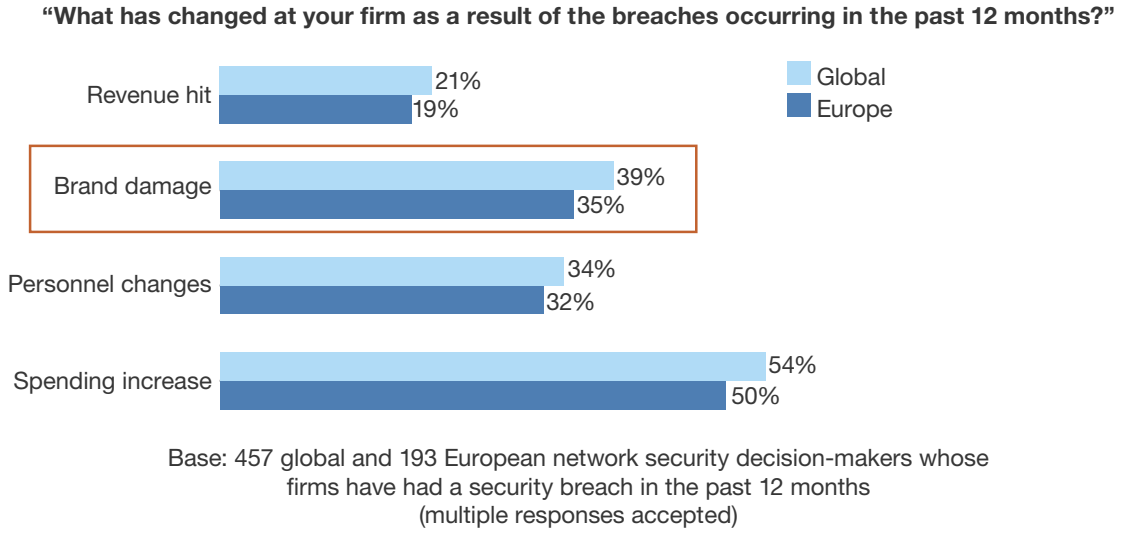
- **Data privacy breaches destroy trust and engagement with your customers . . .** The Edelman Trust Barometer found that customers who distrust a company because of a data breach are likely to criticize that company to family and friends and share negative feedback online; they also abandon companies that they no longer trust.[5] It's not just consumers who are turning a critical eye on these companies; regulators are also getting involved. Consumer rights bills in

France and Germany are changing to include basic data protection principles, such as informed consent and purpose limitation. Companies breaching these consumer rights will face expensive and extensive class actions by consumers as well as prosecutions by data protection authorities.[6]

- **. . . and with your business partners, too.** As more and more companies share or sell data to partners in their value chain or with external firms as part of the broader data economy, they must be able to trust their partners' ability to protect that shared data. Professor Dr. Christoph Bauer, CEO of ePrivacy, told us that an increasing number of companies undergo formal certification processes to satisfy their business partners' request for proof that they have put in place high standards for protecting customer data.[7] For a growing number of organizations across Europe, this is a fundamental condition for being included in a value chain.

- **Data breaches compromise your brand's reputation.** Law firm DLA Piper told us, "When clients' enter this office to discuss data protection infringements, their main concern is for everything to remain completely confidential." Some 39% of global decision-makers and 35% of European decision-makers at firms that experienced a data breach in the past 12 months reported damage to their brand (see Figure 2). Data published by the UK Department for Business, Innovation & Skills shows that 10% of UK organizations that suffered a breach in 2013 were so badly damaged by the attack that they had to change the nature of their business.[8]

Figure 2 Data Privacy Breaches Destroy Customer Engagement



Base: 457 global and 193 European network security decision-makers whose firms have had a security breach in the past 12 months (multiple responses accepted)

Source: Forrester's Business Technographics® Global Security Survey, 2014

. . . And Undermine The Customer Life Cycle

Legal uncertainty and concerns over customer data privacy remain obstacles to the complete fulfillment of the Internet of Things' potential in terms of both market opportunity and customer engagement.[9] For example, European vendors like T-Systems told us that additional regulation for health-connected devices would help reassure skeptical customers and inject more confidence into the market. In all geographies, failing to meet your customers' expectations for data protection will mean that you miss the opportunity to build long-lasting engagement with them.[10] In markets where personal data protection regulations are particularly stringent, like Europe, firms must be particularly careful.[11]

However, our research shows that consumers' data privacy concerns regarding connected devices have the potential to negatively affect the customer life cycle, regardless of whether these devices meet specific legal compliance requirements.[12] CIOs should be aware that (see Figure 3):

- **Customer data protection starts with a bang in the "buy" phase.** Regardless of specific data privacy laws, the protection of transactional data is a must everywhere.[13] As the volume of digital payments increases, credit card details remain at the top of cybercriminals' wish lists.[14] Credit card data leaked during 2013's Target breach resulted in recent gains for cybercriminals who used it with the new Apple Pay system.[15] This shows how complex the task is for CIOs.[16] To get this stage right, they must help their businesses adopt effective data protection practices and strong security measures across the physical and digital touchpoints in their value chain. They must also comply with sector-specific regulations where necessary.[17]

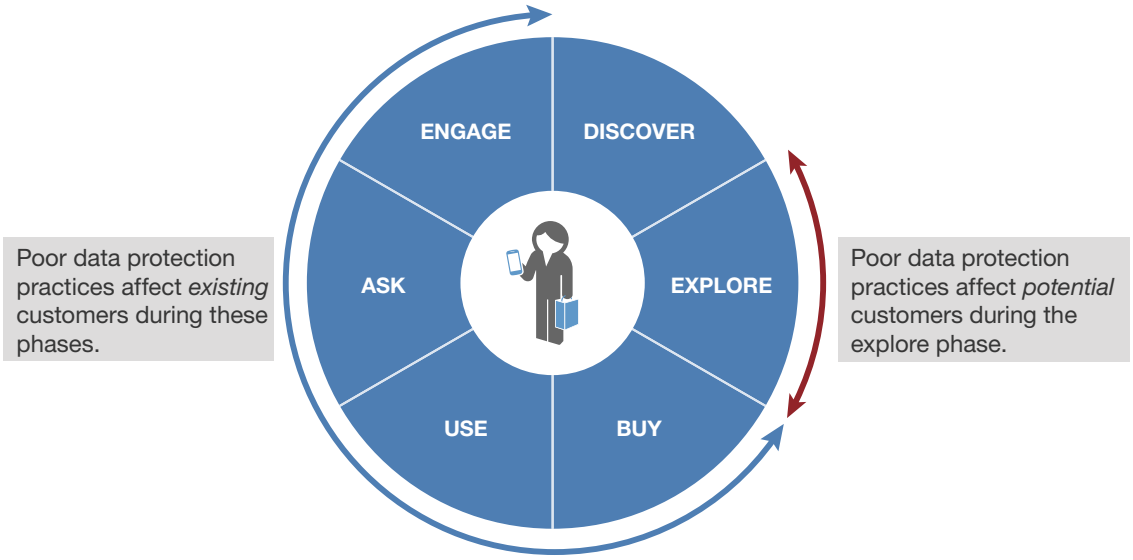
- **Customers test the privacy policy in the "use" phase.** The customer gets her hands on a new fitness tracking device and wants to set it up. This is where she learns about the data that the device will collect about her routine and why — and it's when she consents to it being collected. Getting this communication right is crucial not only to meet compliance regulations but also to inspire confidence in the user, which in turn will affect the subsequent phases of the customer life cycle. However, companies responsible for collecting lifestyle/wellbeing-related data must be aware that the European Union (EU) regulator now considers this category of data to be sensitive, and ad hoc rules apply.[18]

- **Customers exercise their data rights in the "ask" phase.** Customers who agree to share their data may later ask to amend or delete it. These requests involve the entire partner ecosystem with which this customer data is shared. For example, a customer shares her home address and mobile phone number with the grocery store through her connected fridge. The store passes on that data to the delivery company and others in the value chain, such as a partner that will measure the mobile app's performance. If the customer wants to amend or delete her data, the grocery store is ultimately responsible for enforcing the customer's request in all places. This means that the business that "owns" the data bears responsibility for it across the entire IoT value chain, including device manufacturers, developers, connectivity providers, as well as cloud providers and their subcontractors.

- **Customers enter the "engage" phase only if they trust their supplier.** Privacy issues that result in poor interactions with a firm during the previous phases may damage customers' trust and dissuade them from engaging further. Data shows that 68% of customers globally would refuse to buy products or services from companies they did not trust; they also share negative reviews and feedback online.[19] ePrivacy asks its clients to track and share customers' negative feedback with their privacy consultants; in this way, ePrivacy can help its clients measure the effectiveness of their data privacy practices and can provide them with guidance on how to address complaints so that they can mitigate the damage to customer engagement and the brand's reputation.

- **A bad reputation can dissuade prospects in the "explore" phase.** In this phase, prospective customers identify vendors, gather product information, and read online and offline reviews. Bad press or costumer complaints about data protection practices will have an impact in these phases. In 2014, UK B2B and B2C large organizations increasingly experienced extensive, adverse media coverage of privacy breaches and customer complaints.[20] And it's not just prospects who are put off by bad press: Business buyers who assess a business' reputation formally as part of the procurement process could exclude companies from their value chain if they have a reputation for handling customer data poorly.

Figure 3 Poor Data Protection Practices Undermine The Customer Life Cycle



119904 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

EMPLOY EFFECTIVE DATA PROTECTION TO ADVANCE YOUR IOT STRATEGY

To push their IoT strategies forward, CIOs must: 1) build and execute on the infrastructure to support the IoT model, 2) engage and influence internal teams — including business leaders — as well as a broad partner ecosystem as they plan for and implement connected technology, and 3) work with their CISO and CPO to ensure that they implement effective data protection practices across technology, systems, and processes (see Figure 4).[21] To contribute to the implementation of effective data protection practices, CIOs must:

- **Make data privacy a priority when deploying technology.** To navigate effectively and safely through massive amounts of data and the complex IoT ecosystem, tech management leaders should promote privacy and data protection from the start.[22] Good data management plays a crucial role, too.[23] Where personal data protection regulation is particularly strict, as in Europe, data management is also very important for compliance: You must allocate data across systems and clearly align purpose and access.[24] Ideally, CIOs should store and process data in dispersed data clusters and grant access rights only to those employees and external partners who actually need it.[25] The allocation of access privileges, checks, and controls (from both a technical and organizational perspective) is even more important role if all of the data sits in a single, broad database.

- **Adopt clear and transparent privacy policies for the Internet of Things.** To achieve effective data protection, CIOs must work with their CSO, CPO, and their teams to address technical and legal challenges.[26] One fundamental aspect is having a clear privacy policy to accompany products and services. Big tech giants, such as Google and Facebook, have recently experienced the pitfalls of having poor privacy policies.[27] Regardless of a device's size, every app running on it must come with a transparent privacy policy, and users must be able to easily set their preferences and find links to other privacy-related material. Even when different members of a family share the same fitness tracker, they should be able to create as many accounts as they need and personalize them with specific privacy features.

- **Collect only the minimum amount of data needed.** The EU regulator and a number of privacy advocates have repeatedly called for data collection to be limited to only necessary data.[28] While this may be a challenge for broad analytics projects, data reduction remains crucial not only for compliance with data protection rules but also for data security and data management. Firms must protect valuable data not only from those with bad intentions but also from poorly trained employees.[29] They must classify data continually and update the policies and procedures attached to it.[30] Adopting a purpose-oriented approach to data collection will help organizations limit the amount of data they collect and help make other data operations more agile.

- **Adopt industry best practices beyond mere compliance.** Regulators are having a hard time catching up with the Internet of Things, and this is causing gaps in their rules. As a result, both the UK Information Commissioner's Office (ICO) as well as the Federal Trade Commission (FTC) in the US have called on industry members to develop and implement best practices for

data protection in IoT-specific initiatives.[31] Among their recommendations: Build data security and data privacy into devices upfront; retain visibility into external providers' security measures and procedures; and continually train employees.[32] In addition, many organizations have made the protection of customer data part of their corporate responsibility strategy.[33]

- **Remember that protecting customer data is good for business everywhere.** A citizen's right to privacy is enshrined in the European Convention on Human Rights.[34] Outdated but still robust regulations protect it, and companies must go to considerable efforts to comply with them — needing broad assessments of their technology setup, organizational arrangements, legal frameworks and practices, and even business planning to get it right.[35] As a result, firms operating in the EU must shape their data protection strategy around these requirements.[36] However, companies that aren't motivated by these compliance requirements should still look at some of the practices implemented by their EU peers when strengthening their data protection strategies.[37] Protecting customer data is good for business everywhere.[38]

Figure 4 The Data Protection Checklist For CIOs Working In The European Union

The spreadsheet associated with this figure contains additional information.

Determine data ownership
☐ Have you determined what portion of the data you own?
☐ Have you classified the data you own as sensitive/personal or personally identifiable/nonpersonal?
☐ Have you tailored your data protection strategy to specific data categories in an efficient manner?
Gather customer consent
☐ Are your communications with your customers on what data you collect transparent and unambiguous?
☐ Are your mechanisms for gathering customers' consent active (e.g., a tick box)?
☐ Is the request for consent highlighted in your terms and conditions (e.g., a different text color)?
☐ Is the privacy policy available in local languages?
☐ Are the subject rights included in the terms and conditions?
☐ Are links to other privacy resources easy to find?
☐ Can users — sharing a device — create different accounts with different privacy settings?
Communicate the purpose
☐ Are your communications on why you collect and process data transparent and unambiguous?
☐ Have your given your customers meaningful opt-out options (e.g., opt out from data processing)?
☐ Have you anonymized data processed for secondary purposes?
Store and process data in the cloud
☐ Have you communicated unambiguously about data storage and/or processing in the cloud?
☐ Are you aware of the geographical location of your cloud provider's HQ and eventual subcontractors?
☐ Have you obtained and reviewed the list of cloud subcontractors?
☐ Have you reviewed your cloud provider's infrastructure security, security measures, and privacy policy?
☐ Do you encrypt your data at rest and in motion? Do you hold the encryption keys?
☐ If data is transferred outside the EU, does your company comply with international data transfer rules?
☐ If data is transferred outside the EU, does your provider comply with international data transfer rules?
☐ If sensitive data is transferred outside the EU, do you comply with specific regulations?
Analyze the data
☐ Are you processing only data for which you have gathered your customers' consent?
☐ Are you processing data for the purpose you stated in your terms and conditions?
☐ Are you collecting and processing only the data that you need to?

119904 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 4 The Data Protection Checklist For CIOs Working In The European Union (Cont.)

Share data with third parties
☐ Have you communicated unambiguously to your customers about sharing data with third parties?
☐ Have you organized your data in dispersed data sets?
☐ Have you given third parties access only to the portion of data they need?
☐ Are third parties handling data for the purpose stated in your T&Cs or for compatible purposes?
☐ Have you anonymized data shared with third parties for processing other than for the main purpose?
Feed data into social media
☐ Do you gather permission from customers each time you feed data into/derive data from social media?

119904 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

WHAT IT MEANS

THE INTERNET OF THINGS MAKES YOUR TECH MANAGEMENT MORE VISIBLE

Businesses will increasingly depend on data from a variety of different sources, whether it's produced internally across departments, generated by partners in the value chain, bought from external data originators and integrators, or collected from customers. In return, each business will give data back to the ecosystem in a continuous exchange.[39] For this ecosystem and the Internet of Things to flourish, trust, transparency, and interoperability across platforms will be essential.[40] CIOs must:

- **Become interdepartmental orchestrators to ensure effective data strategies.** Siloed organizations will have a hard time achieving success. Silos hinder business agility, collaboration, and alignment across departments; delay digital transformation; and affect the ability to innovate. These organizations also adopt a siloed approach to data, which will increasingly undermine the effectiveness of data consumption and make the CIO's life very difficult when it comes to data management, security, and compliance. The CIO must become an interdepartmental orchestrator and craft her business technology agenda to enable a data-as-a-service approach, where data runs seamlessly across the organization via curated data products and services.

- **Manage broader but more agile value chains.** The Internet of Things multiplies connections and will, over time, make the value chain broader and more interconnected. As data generators, customers will become part of that value chain, too. As a matter of urgency, the CIO will need to achieve full interoperability between platforms and greater agility across technology, systems, and processes.[41] When building a partner ecosystem, the CIO must decide which components can be easily integrated, which can be consumed on

an as-a-service basis, and which must be avoided. Shorter but more frequent interactions with a changing portfolio of providers, open-platform-based technology, and more opex investments will become the rule.

- **Recognize that a wider audience will assess their data protection success.** Traditional IT serves internal employees exclusively. Business technology's reach is much broader, as it includes customer- and partner-facing technologies and systems, so the outcomes of initiatives in these areas will become increasingly visible to these external audiences.[42] CIOs must keep this in mind when developing data protection strategies, especially if operating under strict data protection rules: Failure here will become more and more evident to their partners and customers. As data protection plays an increasingly relevant role in customers' purchasing decisions and business' wider strategies, the business and the broader partner ecosystem will scrutinize tech management's data protection strategies.

SUPPLEMENTAL MATERIAL

Survey Methodology

Forrester's Business Technographics® Global Networks And Telecommunications Survey, 2014 was conducted using a mixed methodology phone and online survey fielded in April 2014 of 3,140 business and technology decision-makers located in companies with two or more employees.

Forrester's Business Technographics Global Security Survey, 2014 was conducted using a mixed methodology phone and online survey, fielded in April and May 2014, of 3,305 business and technology decision-makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics provides demand-side insight into the priorities, investments, and customer journeys of business and technology decision-makers and the workforce across the globe. Forrester collects data insights from qualified respondents in 10 countries spanning the Americas, Europe, and Asia. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

Companies Interviewed For This Report

DLA Piper

ePrivacy

FireEye

Symantec

T-Systems

Telefónica

Tune

ENDNOTES

[1] For a ranking of the maturity of the IoT market opportunity by industry and application, see the "Mapping The Connected Word" Forrester report.

Many vendors have also estimated the market opportunity of the Internet of Things. Cisco, for example, estimates that the IoT market's value will reach $14.4 trillion in the next 10 years, as a result of higher revenues and lower costs. Source: Joseph Bradley, Joel Barbier, and Doug Handler, "Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion," Cisco, 2013 (http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf).

[2] After a wave of IoT adoption aiming mainly at greater efficiencies, businesses are now working to implement platforms that will leverage connected devices for business advantage, focusing on industry-specific needs. For more information about the second phase of implementation of the Internet of Things, see the "Predictions 2015: Software Platforms Drive Internet-Of-Things Adoption" Forrester report.

[3] As shown by the percentage indicating it is a high or critical priority; please note that numbers have been rounded. Source: Forrester's Business Technographics Global Networks And Telecommunications Survey, 2014.

[4] This blog post provides an example of the effect of the Internet of Things on customer data privacy. Source: Fatemeh Khatibloo, "Google's Nest Acquisition Will Force the Internet of Things Privacy Discussion," Fatemeh Khatibloo's Blog, January 15, 2014 (http://blogs.forrester.com/fatemeh_khatibloo/14-01-15-googles_nest_acquisition_will_force_the_internet_of_things_privacy_discussion).

For more insights into how organizations are preparing to address the security needs of the Internet of Things, see the "Prepare Your Security Organization For The Internet Of Things" Forrester report.

[5] Regardless of regulators' specific legal compliance requirements, businesses everywhere should be aware of the emotional intensity of privacy and how this shapes their relationship with customers. For more insight and guidance on how to assess your firm's broad data protection strategy, see the "Measure The Effectiveness Of Your Data Privacy Program" Forrester report.

The 2015 Edelman Trust Barometer found that countries with higher trust levels overall also show a greater willingness to trust new business innovations. Building trust is essential to successfully bringing new products and services to market, and building trust in new business innovations requires that companies

demonstrate clear personal and societal benefits, behave with integrity, and engage with customers and stakeholders throughout the process. Source: "2015 Edelman Trust Barometer," Edelman (http://www.edelman.com/insights/intellectual-property/2015-edelman-trust-barometer/).

[6] Source: "German Government Adopts Draft Law Regarding the Enforcement of Data Protection Law by Consumer Protection Associations," Hunton and Williams, February 6, 2015 (https://www.huntonprivacyblog.com/2015/02/06/german-government-adopts-draft-law-regarding-enforcement-data-protection-law-consumer-protection-associations/) and Monika Kuschewsky and Charlotte Ryckman, "European Consumer Legislation and Online Privacy Policies: Opening Pandora's Box?" Inside Privacy, February 9, 2015 (http://www.insideprivacy.com/international/european-union/european-consumer-legislation-and-online-privacy-policies-opening-pandoras-box/).

[7] Source: Forrester interview.

[8] This survey sets out the number and nature of information security breaches experienced by UK businesses in 2013. The report compares this data with the 2013 information security breaches survey, which looked at breaches in 2012. This shows the scale of cybersecurity threats facing business and how these have increased. It shows how the average number of breaches has risen for both large and small businesses. Small businesses in particular experience higher levels of attacks from outsiders. The survey covers: the number of information security breaches experienced by UK businesses; the type of breach; and the financial cost of these breaches. Large organizations are defined as those with more than 250 employees; small organizations are those with 250 employees or fewer. Source: "Information security breaches survey 2014," Gov.UK, July 3, 2014 (https://www.gov.uk/government/publications/information-security-breaches-survey-2014).

Our research shows that firms pay less attention than they should to customer-facing risks including data privacy. For guidance on how to mitigate customer-facing risks, see the "Mitigate Risks In The Customer's Journey" Forrester report.

[9] Source: David Mayer, "Internet of things needs global privacy push, says UK regulator," Mymeedia (https://mymeedia.com/stages/tech/post/7025362) and Iain Monaghan, "Internet of Things: beware the legal pitfalls," Computing, December 15, 2014 (http://www.computing.co.uk/ctg/opinion/2386833/internet-of-things-beware-the-legal-pitfalls).

[10] In the US, for example, legal compliance with data protection legislation focuses on limited categories of personal data, like health-related data or financial data. Standards are generally agreed with or led by the private sector and are often adopted on a voluntary basis. Nonetheless, customer data privacy is considered the most important and emotional issue when it comes to a firm's security strategy. See the "The New Privacy: It's All About Context" Forrester report. To assess your firm's broad data protection strategy, see the "Measure The Effectiveness Of Your Data Privacy Program" Forrester report.

For an update on US data privacy, see the "Quick Take: The State Of Privacy In The Union" Forrester report.

[11] For more details about how companies should protect their assets and customers' trust, see the "Top Security And Risk Priorities For The Business Technology Agenda" Forrester report.

[12] Tech management must embed controls directly into customer-facing products and services as a competitive differentiator; it must also identify, analyze, and mitigate risks in the customer life cycle and related initiatives. This report provides a framework for identifying security and risk roles and responsibilities at every phase in the customer life cycle as well as the strategies, policies, and technologies to prioritize as part of incorporating data protection considerations into the company's BT agenda. See the "Top Security And Risk Priorities For The Business Technology Agenda" Forrester report.

For guidance on how to mitigate customer-facing risks in the customer journey, see the "Mitigate Risks In The Customer's Journey" Forrester report.

[13] Forrester has created a data privacy heat map that highlights the data protection guidelines and practices for 54 different countries. See the "Forrester's 2014 Data Privacy Heat Map" Forrester report.

[14] For more information, see the "The Cybercriminal's Prize: Your Customer Data And Competitive Advantage" Forrester report; see the "The Future Of Mobile Wallets Lies Beyond Payments" Forrester report; see the "US Mobile Payments Forecast, 2014 To 2019" Forrester report; and see the "Forrester Research Mobile Payments Forecast, 2014 To 2019 (EU-7)" Forrester report.

[15] Source: Robin Sidel and Daisuke Wakabayashi, "Apple Pay Stung by Low-Tech Fraudsters," The Wall Street Journal, March 5, 2015 (http://www.wsj.com/articles/apple-pay-stung-bylow-techfraudsters-1425603036).

[16] For more information about the security of electronic payments and how companies will address this and other security challenges in 2015, see the "Predictions 2015: Security Budgets Will Increase, As Will Breach Costs, Fines, And Lawsuits" Forrester report.

[17] Source: "E-money," European Commission (http://ec.europa.eu/finance/payments/emoney/index_en.htm).

For more information on data security breaches in the payments sector, see the "Predictions 2015: The Quest For Security Will Dominate The Payments Marketplace In The US" Forrester report.

[18] Source: "mHealth in Europe: Preparing the ground — consultation results published," European Commission press release, January 12, 2015 (https://ec.europa.eu/digital-agenda/en/news/mhealth-europe-preparing-ground-consultation-results-published-today).

[19] Source: "2015 Edelman Trust Barometer," Edelman (http://www.edelman.com/insights/intellectual-property/2015-edelman-trust-barometer/).

[20] Source: "Information security breaches survey 2014," Gov.UK (https://www.gov.uk/government/publications/information-security-breaches-survey-2014).

[21] For more information about how CIOs can build and operate the infrastructure necessary to support the Internet of Things, see the "Brief: CIOs Will Architect And Operate The Internet Of Things" Forrester report and see the "Smart Products Will Require A Hybrid CTO/CIO Skill Set" Forrester report.

Beyond compliance, the Internet of Things requires firms to adjust their security strategy to meet the needs of the connected world. For more details, see the "Prepare Your Security Organization For The Internet Of Things" Forrester report.

[22] "Privacy by design" is an approach that aims to promote the adoption of measures that protect privacy and data protection from the start of any IoT project. Source: "Privacy by design," ICO (https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/).

[23] With more and more data touching internal firms' platforms, data management is becoming more important than ever, as is allocating responsibility for it across tech management teams. For guidance on the right allocation of responsibility for data management, see the "Eliminate Confusion In Data Management Roles And Responsibilities" Forrester report.

For guidance on building a data management strategy that addresses the challenges of the Internet of Things, see the "Design Tomorrow's Data Management For Agility In Context" Forrester report.

[24] For an overview of identity and access management technologies, see the "Navigate The Future Of Identity And Access Management" Forrester report.

[25] CIOs might also consider the adoption of privileged identity management (PIM). PIM ensures that only authorized employees can access high-risks environments and creates irrefusable and tamper-proof evidence for sensitive system access. For more details, see the "Critical Questions To Ask Your Privileged Identity Management Solution Provider" Forrester report and see the "Lessons Learned From Global Customer Data Breaches And Privacy Incidents Of 2013-14" Forrester report.

[26] To assess the role of the chief privacy officer in the wider business data protection strategy, see the "Brief: What Keeps Privacy Pros Up At Night?" Forrester report.

[27] Source: Samuel Gibbs, "Facebook's privacy policy breaches European law, report finds," The Guardian, February 23, 2015 (http://www.theguardian.com/technology/2015/feb/23/facebooks-privacy-policy-breaches-european-law-report-finds) and "Google privacy policy found to breach EU data protection law," White & Black (http://www.wablegal.com/e-bulletin/nullam-dictum-felis-eu-pede-mollis-pretium-integer-tincidunt).

[28] Source: "Article 29 Working Party," European Commission (http://ec.europa.eu/justice/data-protection/article-29/index_en.htm).

[29] Forrester defines human-factor-friendly (HFF) security as the act of analyzing and addressing the impact of human factors on the success of security controls in applications, products, or services that the enterprise deploys to its own workforce or to its customers. Success is a measure not only of the effectiveness of the control to mitigate threats to an acceptable level of risk tolerance set by business owners but also a measure of its effectiveness as compared with its impact on user experience. In this report, we review human factor successes and failures and help security leaders understand the success contributors and resistors that will help them raise the bar on all the security products, solutions, and programs that they choose to implement. See the "Raise The Security Bar With Human-Factor-Friendly Design Concepts" Forrester report.

[30] Defining data via data discovery and classification is an often overlooked, yet critical, component of data security and control. This report outlines common challenges, data classification roles, and approaches to data classification. See the "Rethinking Data Discovery And Data Classification" Forrester report.

[31] Source: "FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks," Federal Trade Commission press release, January 27, 2015 (https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices) and "Ofcom sets out plans to support the Internet of Things," Ofcom, January 27, 2015 (http://media.ofcom.org.uk/news/2015/iot-next-steps/).

[32] To build a strong data protection strategy, regardless of compliance requirements, see the "Predictions 2015: The Governance, Risk, And Compliance Market Is Ready For Disruption" Forrester report.

[33] For further details on how organizations are complying with customer demands by implementing and reporting on responsibility initiatives, see the "Meet Customers' Demands For Corporate Responsibility" Forrester report.

[34] Source: "European Convention On Human Rights," European Court of Human Rights (http://www.echr.coe.int/Documents/Convention_ENG.pdf).

[35] For more information on privacy, see the "Customer Privacy Is A European CIO Priority" Forrester report.

[36] ePrivacy provides an example of the technical and legal arrangements necessary to comply with the EU's personal data protection regulations. Source: "ePrivacyseal," ePrivacy, November 2013 (http://www.eprivacy.eu/fileadmin/Redakteur/pdf/EPS_criteria_EU_catalogue_nov2013.pdf).

[37] For guidance, see the "Predictions 2015: The Governance, Risk, And Compliance Market Is Ready For Disruption" Forrester report.

[38] For more insight into how businesses are gaining a competitive advantage through strong data protection and security strategies, see the "Predictions 2015: Data Security And Privacy Are Competitive Differentiators" Forrester report.

For guidance on how to assess your firm's broad data protection strategy, see the "Measure The Effectiveness Of Your Data Privacy Program" Forrester report.

[39] The connected world creates a data economy with consequences for firms' internal operations and strategic planning as well as for their competitive landscape. For more details, see the "Mapping The Connected Word" Forrester report.

[40] After a wave of IoT adoption aiming mainly at greater efficiencies, businesses are now working to implement platforms that leverage connected devices for business advantage, focusing on industry-specific needs. For more information about the second phase of implementation of the Internet of Things, see the "Predictions 2015: Software Platforms Drive Internet-Of-Things Adoption" Forrester report.

[41] While many IoT implementations are driven by business leaders and other groups, technology management teams are the ones ultimately responsible for operating the resulting infrastructure. For more details about the new technology architecture that CIOs must build and operate to address the new requirements of the Internet of Things, see the "Brief: CIOs Will Architect And Operate The Internet Of Things" Forrester report.

[42] For more information, see the "The CIO Mandate: Engaging Customers With Business Technology" Forrester report.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On CIOs

As a leader, you are responsible for managing today's competing demands on IT while setting strategy with business peers and transforming your organizations to drive business innovation. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.