INTRODUCING DIGITAL TRUST INSIGHTS

by Vitaly Sokolov
Partner, PricewaterhouseCoopers Russia

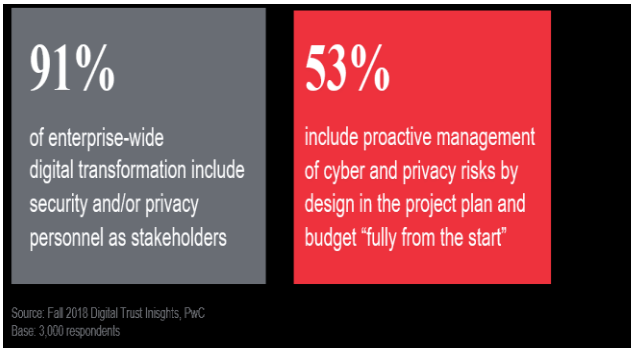
For 20 years, leaders have turned to PwC's *Global State of Information Security® Survey (GSISS)* as a trusted resource to navigate the cyber risk landscape. Over time, that landscape has evolved to be less about "information security" and more about managing digital risk. As cybersecurity, privacy, and data ethics become increasingly intertwined, organizations need an authority for research data and actionable advice. That is why PwC is rebooting GSISS to create Digital Trust Insights. This new platform will explore how to build confidence in the readiness of people, processes, and technologies to meet tomorrow's challenges.

Engage security experts at the start of digital transformations

Companies everywhere are pursuing digital transformation projects—putting emerging technology into action while aiming to solve problems, create unique experiences, and accelerate business performance. It's no secret that sprawling connectivity among personal devices, governments, businesses, and industrial equipment is fueling exponential growth in cyber and privacy risks.

Nine out of ten GSISS survey respondents at companies executing digital transformation projects say that security and privacy personnel are included as stakeholders and that their companies proactively manage cyber and privacy risks by design (within a project's plan and budget).

However, only 53% say that proactive risk management measures are integrated into the project "from the start." That percentage is higher in the financial services, health, and TMT[1] sectors and is lower in consumer markets (among respondents from medium and large companies). With this in mind, there is not one company here that does not have the opportunity for improvement – businesses worldwide can do better.


91%

of enterprise-wide digital transformation include security and/or privacy personnel as stakeholders

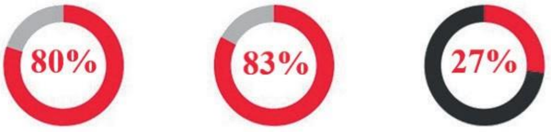
53%

include proactive management of cyber and privacy risks by design in the project plan and budget "fully from the start"

Source: Fall 2018 Digital Trust Inisghts, PwC
Base: 3,000 respondents

Improve communications and engagement with the board of directors

Most respondents responsible for communicating with the board on cyber and privacy risks say that their company has provided the board with strategies for cybersecurity (80%) and privacy (83%). Many of these same businesses, however, may have doubts or concerns around their internal reporting on cybersecurity and privacy metrics. Only 27% of respondents say that they are very comfortable that the board receives adequate reporting on metrics for cyber and privacy risk management.



say the board has been provided a cyber risk management strategy

say the board has been provided a privacy risk management strategy

say they are "very comfortable" the board is getting adequate reportin on metrics on cyber and privacy risk management

Source: Fall 2018 Digital Trust Inisghts, PwC
Base: 3,000 respondents

<u>Actionable advice for business leaders</u>

1. Know that the types of measures (implementation, effectiveness/efficiency, and impact) that are obtainable and useful for performance improvement depend on the maturity of the security program and how controls are implemented. Start with what can be measured today and create a plan to add more sophisticated metrics over time.

2. Also, metrics must address the needs of the stakeholder audience. The board might want metrics on the business impact of security activities—for example, the impact of security spending on overall risk posture, the cost of addressing a security event, or the impact of security efforts on public trust.

3. Communicate to the board how external factors—threats, third-party risk and regulations—affect overall risk posture and effectiveness of risk reduction.

4. Improve the CISO's[2] engagement with the board

Boost cyber resilience

Cyber resilience includes the agility of both defense and recovery capabilities. Resilient systems help companies sustain operations when possible amid cyberattacks and help rapidly recover in the event of a disruption. This is critical because crippled operations can lead directly to financial losses that often exceed, and mount more quickly than those from data exposure.

[1] Technology, Media, and Telecommunications

[2] Chief Information Security Officer (CISO)

The importance of maintaining data integrity will only grow as companies make more data-driven decisions with the aid of artificial intelligence. Only about half of medium and large businesses in key sectors say that they are building resilience to cyberattacks and other disruptive events, and fewer than half say that they are very comfortable that their company has adequately tested its resistance to attacks.

Actionable advice for business leaders:

1. Develop an understanding of the risk appetite around core business practices. Take into account the different views of stakeholders such as the chief financial officer, the chief operating officer, the chief information officer, and other executives focused on security, privacy, and risk.

2. Use leading approaches to cyber resilience. This includes developing and assessing plans designed to address risk-appetite concerns in an evolving threat landscape. It should also include monitoring the technology infrastructure to enable high availability, disaster recovery, and data integrity.

Be proactive in compliance

Respondents say that the greatest important challenges in digital compliance and ethics worldwide include the awareness of the latest regulatory developments (41%), compliance with current regulations (37%), and preparedness for future regulations (34%). Brazil's data protection law is a recent example of new legislation. Perhaps the most well-known example is the European Union's *General Data Protection Regulation (GDPR),* which went into effect in May 2018. Fewer than half of all companies worth $100 million or more that responded say that they are fully ready to comply with the GDPR.

Among US respondents, confidence about the readiness to comply with the *California Consumer Privacy Act*—which goes into effect in 2020—varies by sector: TMT companies are the most confident and health companies are the least confident. Three-quarters of respondents in China say they are entirely ready to comply with China's cybersecurity law, but far fewer respondents in other countries assert the same.

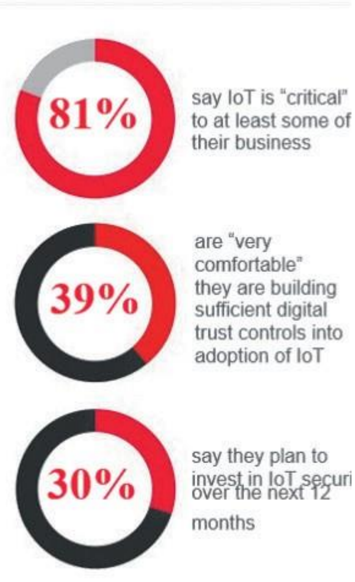
Actionable advice for business leaders:

1. Focus more on identifying new and emerging legislation, rules, and guidance on their implementation.

2. Use an integrated compliance approach instead of siloed efforts. In other words, businesses operating across different jurisdictions should comply with the highest standard. The boundaries of such an approach should be the sum of all the rules.

Accelerating controls for emerging technologies

Keep pace with innovation



Source: Fall 2018 Digital Trust Inisghts, PwC
Base: 3,000 respondents

Explosive growth in technology and data over the next decade will obliterate barriers between the cyber, physical, and virtual worlds, thus ratcheting up the complexity and scale of cyber and privacy risk management worldwide. Digital data and devices will be embedded more into critical infrastructure, consumer products, vehicles, daily life, and even in humans themselves, in a "world in which the physical, cyber and virtual merge." Data collection will be more pervasive than ever as the internet of things (IoT) spreads like ivy—and hackers will be drawn to its vines like birds to its berries. Not surprisingly, most respondents (81%) say IoT is critical to at least some of their business. Only 39%, however, say they are very confident they are building enough "digital trust" controls—security, privacy, and data ethics—into their adoption of IoT.

In addition, only 30% list IoT security among the safeguards they plan to invest in this year. IoT devices interact with the physical world in novel ways. These devices often cannot be accessed, managed or monitored like other information technology, and they sometimes require additional cybersecurity and privacy controls.

Survey respondents have even less confidence in their digital trust controls for other emerging technologies such as artificial intelligence (AI). The allure of AI as an essential tool with a multitude of uses, such as predicting the rise of pandemics, driving autonomous vehicles, and augmenting cybersecurity measures, will pressure companies to implement it.

According to the survey, 70% of respondents say AI is critical to at least some of their business, but only 31% are very comfortable they are building enough digital trust controls into their adoption of it. Also, only 22% of all respondents say that they plan to invest in AI as a security safeguard over the next year. This percentage, however, is higher among medium and large companies as in TMT (46%) and financial services (40%). Such investments could one day transform the role of the CISO and provide ways to defeat otherwise unstoppable AI-powered cyberattacks and deception schemes.

Companies that commit to building and demonstrating new trust mechanisms in the crucible of today's business, risk management, and compliance challenges will likely define tomorrow's digital economy, crowding out less dedicated competitors.

Actionable advice for business leaders

1. Prioritize the development of digital trust controls and security budgets to support business investments and objectives around IoT, AI, and other emerging technologies.

2. Stay attuned to emerging IoT security research. For instance, Carnegie Mellon University (CMU) researchers at the Risk and Regulatory Services Innovation Center at CMU have been researching the development and design of new threat modeling, risk, and maturity assessment frameworks for IoT. Such frameworks could enable organizations to make more informed decisions about which actions and controls to implement for IoT security.

3. When creating software, do not simply integrate development and operations but embed security in the process (DevSecOps).

4. Recognize that AI will need both more robust governance and a new operating model.

5. Recognize that emerging research in quantum computing could have profound implications for cybersecurity. It is never too early to begin preparing.