

Digital Transformation and Data Privacy



Contents

03	Executive summary
04	Digital transformation
04	Organizations
04	People
05	The Challenge for Business
06	What Happens when Trust is Lost?
07	Data Security as a Boardroom-Level Issue
08	Compliance
08	Some New and Changing Laws and Regulations
08	Compliance Is Not Enough
09	What Is Best Practice?
09	Encrypt everything
10	End-to-End Encryption
10	Conclusion

Executive summary

Digital transformation continues to have a huge positive effect on both organizations and individuals. Among many advances, it has certainly made commerce easier. But commerce is based, in part, on trust by purchasers that their data will not be misused to cause them harm or inconvenience. This makes the commercial aspect of the digital transformation dependent on the security of purchaser data. Organizations around the world that have taken this issue lightly have suffered as a result, and boards of directors have taken note.

Compliance with governmental regulations and industry standards remains the number one driver for data protection strategies, such as encryption, but new and changing regulations are added daily creating a patchwork of compliance challenges for organizations that operate internationally or even that deal with personal information from multiple countries. In addition, compliance regulations generally lag behind digital security threats in the actual marketplace.

Thales believes the greatest asset for most commercial organizations is their relationship with their customers. And while compliance is a critical first step, it is unfortunately not enough to keep customer data, and the organization's relationship with those customers, safe from cyber criminals.

Thales offers a suite of data protection technologies that are state of the art for protecting the data itself through advanced encryption and managing and monitoring access to the encrypted data. An ever more cost-effective strategy for enterprises dealing with geometrically increasing amounts of data, which is frequently difficult to classify as sensitive or not, is to encrypt everything. Thales can encrypt your data in place behind the scenes and with zero downtime making an encrypt-everything strategy more appealing than ever. End-to-end encryption adds the encrypt-everything concept to point of sale.

Digital transformation

The digital transformation of business is more than a buzzword. It is a reality—not only for organizations in every sector around the world, but for all the people with whom these organizations interact.

Organizations

In 2016, we saw organizations increasingly invest in a digital transformation strategy and CIOs have continued to drive that change through 2017. Gartner's 2017 CIO agenda survey found that more money is being invested in technology that supports shifts to digital services than in the past. At the same time, boards are increasing the pressure on CIOs to move the organization forward technologically to better compete in this ever-increasingly digital world.

Digital transformation is moving the business (and the CIO's job) away from a technology management and instead looking to technology to drive the business forward. Whether that means migrating a company's data center to the cloud, putting an increased focus on analyzing data or defining the organizational culture to work more digitally, businesses are not taking this transformation lightly. Organizations have found that becoming a digital enterprise enables them to be smart, agile, dynamic, fast and competitive, and this agility allows them to better serve customers.

People

People's lives have been digitally transformed as well. We shop by doing online research and comparing prices online before deciding whether we want to buy online or in a brick-and-mortar store. And, if we want the brick-and-mortar experience, we may well check online to be sure the product we seek is in stock or to have it waiting for us when we arrive.

Students have gone from receiving and handing in assignments on Blackboard to attending lectures online, downloading and reading texts on mobile devices, uploading assignments, and getting degrees virtually. In grade school, research assignments frequently involve online searches. And some classrooms visit with other classrooms, authors and experts on other continents via technologies, such as Skype.

Which brings us to the multitude of modes for social interaction through technology. We may not be able to get our children to talk with us via their mobile phones, but they will usually text back if we text first. And when they leave the nest, for whatever reason, we can use technologies like Skype and Facetime to stay in touch.

People with relatively rare interests come together in online communities. So, too, do people with an interest in organizations come together to air their likes and dislikes online, and these thoughts become fodder for traditional and new media.

The digital transformation has made major inroads into how we spend our downtime as well, enabling us to listen to and view media from around the world from anywhere we can get a digital connection. We can even attend worship services online.

Then there is the Internet of things (IoT). Laptops, tablets, smartphones, thermostats, fitness trackers, insulin pumps, cars, industrial applications too numerous to mention here. And this is just the beginning. More and more connected devices come online daily, generating more and more applications and exponentially more data.

The ways in which the digital transformation has affected the way we work are too varied, diverse and numerous to even begin to discuss here. But if you have a job, you can undoubtedly look around you, while at work, and see example after example of work activities you do differently today than you did a few years ago.

The Challenge for Business

For most organizations, the advantage of digital transformation is or will be the ability to execute commerce more fluidly than their competitors can—to achieve the agility we spoke of above.

However, to do this, organizations must also defend themselves against the single greatest threat the digital transformation poses: data that is not secure.

Data security enables commerce

As we know, commerce takes place when two parties—for example, an organization and a customer—agree to make an exchange of currency for goods and services. In our digitally transforming age, this exchange generally requires the purchaser to provide information to enable the currency exchange. But that purchaser expects the information not to be used for unauthorized transactions. The purchaser trusts the organization to protect and not misuse that information. If the customer does not have that trust in the organization, he or she will take his or her business elsewhere.

Customers expect the organizations with which they do business to keep their information secure. Similarly, when a medical organization collects information about a specific patient, the patient agrees that information can be used only for specific purposes. That patient expects the information to be protected, so it cannot be used for other reasons. If the information is not protected, the patient may be able to sue, and go to other providers. And he or she can certainly complain to regulators that his or her privacy has been invaded.

Trust

We at Thales talk a lot about trust. It's a term of practice that describes what our products and services provide our customers. By protecting their data through encryption, tokenization, key management, hardware security modules (HSMs), digital signing and consulting services, we help our customers protect the data with which they are entrusted. We enable them to be trustworthy partners in commerce, health care and more. But, this means going beyond compliance to best-practice security.

What Happens when Trust is Lost?

There may be those among you who would argue this trust is not necessary or that our emphasis on it is overblown. Let's consider some organizations, which were cavalier about keeping their end of the trust compact with their stakeholders.

U.S. hacks

Target proves fallible

Following its 2013 breach, Target was forced to pay consumers \$10 million. The company also reached a \$67 million settlement with Visa, which was brought on behalf of Visa cardholders affected. In December 2015, it was announced Target had agreed to settle with MasterCard for \$39 million. While this might not seem like very much given the sheer size of the company and revenue it brings in, it is likely this isn't the end of Target's data breach payouts.

If you think Target's woes are purely financial, think again. Since the breach, the company has contended with lost sales, diminished customer goodwill and diminished trust. To be fair, the company was grappling with growing pains prior to the breach—but the attack unfortunately made the situation even worse.

Home Depot misses the mark

In September 2014, Home Depot reported 56 million credit cards were potentially affected by a breach spanning five months. According to reports, prior to the breach Home Depot had started encrypting its payment terminal data but was outpaced by the hackers. Around one year later, SC Magazine reported the "expected cost to Home Depot for a cyber intrusion may reach into the [\$]billions."

Perhaps even more damning than the cost was the backlash against the company. In May 2015, consumers filed a 187-page complaint against Home Depot. In it, they cited "overarching complacency when it came to data security." "Complacency" and "business" should never be used in the same sentence—unless one is referring to a trait that hampers success.

Needless to say, subsequent lawsuits against Home Depot have clearly illustrated a breach in trust between the company and its customers. As we all know, building trust takes time. Tina Stewart described it perfectly in her [December 2015 blog](#) about the second anniversary of the Target breach: Successful retailers understand the strategic advantage of what is called "lifetime value" in terms of the consumer. And nothing destroys lifetime value more quickly than lack of consumer confidence. For retailers, protecting customers' information this holiday season, and all year long, has become a large part of maintaining this confidence.

International hacks

Data security is not just a U.S. issue. [An InfoWatch study](#) found that in 2016, Russia registered 213 confidential data breaches, which put the country in second place, just behind the U.S. The U.K. is third. Unfortunately, those are only the top three countries for this kind of data security breach.

The VTech hack: getting personal

One example of a recent international breach that raised hackles—and with very good reason—was the attack against Hong Kong-based company VTech. Here's why:

- Stolen data included private information of over 5 million parents, and profiles of over 6 million children (including chat logs, kid's photos and more)
- Additional compromised data included names, addresses, emails, IP addresses, secret questions and answers for passwords
- The affected are children, a particularly vulnerable segment of the population

Members of the press scorned VTech's January 2016 announcement that it was unveiling a home monitoring system. Understandably, they didn't hesitate to point out the irony of this strategy. Boing Boing's Cory Doctorow was particularly biting, writing "Remember the Hong Kong-based crapgadeteer Vtech, who breached 6.3 million kids' data from a database whose security was jaw-droppingly poor (no salted hashes, no code-injection countermeasures, no SSL), who then lied and stalled after they were outed? They want to make home security devices that will know everything you say and do in your house."

CEX: Whom will you trust to keep your data safe?

British games and electronics retailer CEX recently suffered a breach of the details of 2 million customers including names, addresses, email addresses and some phone numbers, as well as a small number of encrypted credit card details. While it's too early to say what the overall impact on CEX will be, Raj Samani, chief scientist and fellow at McAfee noted in [TProPortal.com](https://www.proportal.com):

- ...Two million people will now be wondering just what the lasting impact of their personal data being disclosed will have on them. ...One lesson is clear, however, anytime you are asked for your personal data either online or offline, question whether you want yet another party to become responsible for keeping it safe.

The common denominator

What do the companies above all have in common? There are a number of thoughts that come to my mind, but for the purpose of this blog, I'm focusing on one big one: they failed to protect the data of people who trusted them to do so.

Data Security as a Boardroom-Level Issue

Considering the effect these data security catastrophes have had on the businesses that experienced them, it is no surprise that data security has become a board-level issue.

Traditionally an organization's encryption strategy would have fallen primarily within the confines of its IT team. However, findings from Thales's 2017 Global Encryption Trends Study show that the balance of power has shifted.

For the first time in the history of the study, business unit leaders now have the highest influence over encryption strategy—up from 10 percent in 2005 to 30 percent in this year's study. In contrast, the influence held by IT operations has significantly decreased over the same time period from 53 percent to 29 percent. Increasingly, encryption is becoming a boardroom-level issue.

It's no coincidence that this rise in influence on encryption strategy among business leaders mirrors the rising number of massive data breaches impacting high-profile companies. With such devastating effects to a company's bottom line and reputation, as well as a considerable loss of customers, the risk of falling victim to a data breach is undeniably keeping board members awake at night. Data privacy is now of paramount importance for businesses wanting keep valuable data—both their own sensitive data and that of their customers—out of the hands of a malicious hacker, and becoming tomorrow's headlines.

Today, the stakes are too high for an organization to stand by and wait for an attack to happen before introducing measures such as encryption that are widely recognized as best practices to protect sensitive data. And although the balance of power in terms of driving encryption strategy has changed, the partnership between business leaders and IT operations to ensure that encryption and associated lifecycle management of encryption keys is done well is paramount.

Compliance

To date, compliance remains the number one driver for enterprise encryption strategies. The 2017 Thales Data Threat Report found that almost half (44 percent) of global enterprise organizations list meeting compliance requirements as their top spending priority.

Some New and Changing Laws and Regulations

Top of mind for European organizations and those who do business with them is a new legal framework known as the General Data Protection Regulation, or the GDPR. These new requirements will go into effect May 2018, but 2017 has been an important year to prepare for compliance. This regulatory framework affects every business offering goods or services to EU citizens, regardless of where the company resides.

In Mexico, violations of Mexico's federal law on the protection of personal data held by private parties often lead to high fines and penalties. In fact, the regulation's fines can grow up to 320,000 times the Mexico City minimum wage—and fines at or near this limit have been levied. A recent report found that, despite the financial burden, breaches among Mexican organizations in the last year alone were up more than threefold from the previous year.

In Japan, the country's amended Act on the Protection of Personal Information (APPI) is soon to go into effect. The amended APPI applies to "personal information handling business operators," which is defined as a person providing a personal information database for use in business. Although there are limited exceptions to this definition, certain obligations under the amended APPI will apply to most businesses using a personal information database for their business in Japan, regardless of the place of incorporation. The deadline for full compliance with APPI is May 30, 2017, and Japanese enterprises are making compliance a top IT security spending priority.

Other countries, such as Australia, have recently revised their data protection regulations. The Privacy Amendment (Notifiable Data Breaches) Bill 2016 was passed by the Australian Parliament on February 13, 2017. However, this legislation has been in the works for quite some time now. The bill is primarily focused on data breach disclosure, and will provide Australians with greater clarity about the privacy of their personal information.

China too is in the process of rolling out new cybersecurity regulations and an overarching data protection framework of its own. The new law requires that companies store their data within China, and imposes security checks on companies in sectors such as finance and communications. Although the new regulations aim to strengthen the cybersecurity posture of Chinese companies, data residency laws such as this continue to cause headaches for multi-national businesses and governments handling personal data.

Because there are no internationally agreed laws around data sovereignty, enterprises—which commonly leverage cloud providers and data centers all over the world—are often left facing many unanswered questions.

In the U.S. organizations will be quite familiar with well-known compliance standards such as HIPAA/HITECH, PCI DSS and Sarbanes-Oxley. Organizations required to meet compliance standards are typically those handling vast quantities of personal and financial information, particularly financial, retail and healthcare companies. This data is extremely attractive to cyber criminals and fraudsters.

Healthcare data has become highly desirable to bad actors and much more valuable than credit card information. The enormous detail available in patient records makes it possible for criminals to not only apply for credit cards or loans, but also to generate large sums from fraudulent medical charges—or even to compromise a patient's existing financial accounts.

Compliance Is Not Enough

Unfortunately, compliance is only somewhat helpful in addressing data security. Cyber attacks change daily and hourly, but compliance regimes take many months and years to update. This leaves compliance mandates requiring organizations to use protection methods that attackers may have already circumvented. Compliance is certainly a baseline standard and a good starting point, but it is not a foolproof strategy for protecting sensitive data. And, as we've seen, in the case of a serious breach, being compliant won't save your organization from the financial impact of lost sales, reduced sales price, and a tarnished reputation.

Today we do not think about whether an organization will be breached, but when. Across time a breach is close to a statistical certainty. So the question senior managers should ask is: What is the downside risk for our company of a serious breach?

Have some of your risk management folks do some research and generate some scenarios taking into account lost sales; lost customers; reduced share price; legal settlement costs; the challenge of hiring good staff, and so forth, when your reputation is tarnished. We suspect that if you go through such an exercise, you will quickly agree that it makes sense for your data security to be at best-practice level.

What Is Best Practice?

Unfortunately, Thales cannot provide all that you need to be best practice in data security. That really starts with senior management caring enough about customers, other stakeholders and IP to put in place and enforce the policies necessary to make your data safe from those who would steal or misuse it.

But once management is behind ensuring best-practice data security, Thales can help you put in place many of the technologies that are not only necessary for compliance, but are state of the art for protecting your data. These include:

- Protecting the data itself through encryption and tokenization, so that if the data is breached it will be safe because it will be meaningless to cyber criminals
- User access policy controls, so malicious privileged users or cybercriminals who gain access to credentials can access only limited amounts of data
- Advanced encryption key management, to manage the lifecycle of encryption keys and keep them safe
- Security intelligence logs, which enable organizations to identify breaches in progress
- General purpose hardware security modules (HSMs) that provide a hardened, tamper-resistant environment for encryption, secure cryptographic processing, and key generation and protection
- Payment HSMs, to safely perform tasks such as PIN protection and validation, transaction processing, mobile and payment card issuance, and key management.
- Digital signing to provide verification of the authenticity and integrity of proprietary application code, legal documents, financial records, etc.
- Data in motion encryption hardware to provide high-assurance encryption methods and state-of-the-art key management techniques for maximum protection of sensitive transmissions and assets

Encrypt everything

As we've discussed, internal and external risks and threats to your information are growing every day—in scope, volume and impact. So, while your organization is under increasing pressure to stay competitive and compliant with new regulations, the ultimate goal is ensure the organization's data. Protecting the digital enterprise is more than protection from cyber-threats, it also includes the confidentiality, integrity and availability of your data.

While no organization is immune to the threat of security breaches, implementing data encryption is a major safeguard that will protect information assets and your organization's reputation. Most organizations agree that encrypting sensitive data, particularly data-at-rest (DAR) is a solid data protection strategy. But there is a fallacy in that approach.

First, there is far more data than ever before and it continues to be created at an astounding rate. Often it is presumed that encryption is a painful endeavour, so it is restricted only to the most valuable information assets. This leads to the problem of data classification. Without data classification, you don't know where that sensitive data sits, what interacts with it, or what that data represents to your organization in terms of worth and determining risk. But what constitutes "sensitive?" Not everyone agrees on what "sensitive" means, so organizations have to spend time and energy defining what "sensitive" means for them. This takes a lot of time and resources to implement.

This is no longer the case. In the past, pervasive encryption was largely abandoned, because it was too expensive in time, in its computational requirements, in its space requirements, in its operational efficiency, and in its management and overall ease of use. These technological challenges led to the practice of encrypting only sensitive data. But nearly all of these obstacles have been removed and solved, clearing a path to a simpler, cost-effective encrypt-everything strategy for CSOs.

At Thales, we have made great strides in eliminating the need for downtime to do the initial transformation. We can behind the scenes and with zero downtime transform and encrypt your data in place. So, organizations no longer need to go through the complex, costly and time-consuming exercise of data classification. Encrypting all of your data ensures that you are always in compliance with various regulatory standards and requirements, as data moves around in the organization and even between on-premise and in the cloud.

Just as important, an encrypt everything approach can protect your organization's brand and reputation. Most experts agree that nearly every organization will suffer a data breach at some point—it's a matter of "when" not "if" you'll be attacked. Imagine the peace of mind (and risk reduction) in knowing that any data siphoned out of your organization is encrypted and therefore worthless to the cyber criminal who stole it. Most compliance standards maintain that if your data is encrypted, publicly reporting breached data is not required. Your peers who stick with a sensitive only approach to encryption will need to spend cycles determining, if the breached data was sensitive, and if it was encrypted. If it was not, they will have to report the breach publicly. The damage will extend to the company's brand and reputation in the eyes of customers, partners, potential employees and other stakeholders.

Very smart people at very smart companies have come to the conclusion that encrypting a vast majority of their data is one of the best things they can do to reduce risk and assuage customer fears. While no company or CEO wants to discuss a data breach, having a broad-based strategy to make data protection a priority plays well from both a security and marketing perspective.

An encrypt everything strategy ensures that all data is encrypted and protected by strong access controls such that only those persons with business need to know have access to intended data and only to intended data. Privileged users can be blinded from enterprise data with access only to the metadata, removing the need for data classification. And CSOs are able to assess risk differently by maintaining, modelling and providing access to data in a completely new and different way.

End-to-End Encryption

While “encrypting everything” sounds inclusive, it is usually applied to data at rest. The strategy can and should be extended to include sensitive purchaser data using “end-to-end” encryption.

In end-to-end encryption, data is protected by default wherever it goes over its entire lifecycle. Sensitive data is encrypted the moment it is captured, in a point-of-sale (POS) device at a retail store, for example, and stays encrypted or is re-encrypted while it moves between systems and security domains. This notion of encryption as a data “bodyguard” that always accompanies data objects (files, documents, records, and so on) is appealing but raises questions about establishing trust relationships between different domains and interoperability when it comes to key management.

CISOs and CSOs, who are serious about implementing an end-to-end data protection plan, need to consider how to secure data at each point in its creation, transmission and use. Some critical elements of this are:

- Secure identities—whether personal or for applications and devices
- Secure communications that ensure data isn’t exposed or altered in transit
- Secure storage of information that strongly controls access
- Secure use that only allows authorized users and applications

Each and every one of these elements relies on encryption and other cryptographic technologies, access controls and identity—all of which are offered or supported by the Thales solution platform.

Conclusion

Organizations that want to survive and thrive in this age of digital transformation need every advantage they can get: top talent, top strategies and of course, top technology. Technology, after all, has helped make business transactions faster, more transparent and more efficient. Big data, cloud computing, the “Internet of Things,” robotics, bots and other forms of artificial intelligence are all technologies that your organization is probably considering or reviewing, if they are not already in use.

These technologies also blur or eliminate traditional enterprise perimeters, and present new conduits for cyberattacks as attackers simultaneously are becoming more sophisticated. We live in a world of malware, ransomware, spear phishing, insider threats, nation-state attacks, APTs, SQL injections and social engineering.

There are no “magic bullets” to protect against this reality, but if CSOs and CISOs “follow the money” and focus on an encrypt-everything approach to data protection, they can become enablers for new business and technology use while protecting the data entrusted to them by stakeholders and the reputations and financial strength of the organizations they serve.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.



Americas

2860 Junction Avenue, San Jose, CA 95134 USA
Tel: +1 888 744 4976 or +1 954 888 6200
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific - Thales Transport & Security (HK) Ltd

Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

Europe, Middle East, Africa

Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalescpl.com <

