



Better Security Drives Innovation

Building an overall worldwide security system for the long term



EXECUTIVE SUMMARY

You learned it in school. During the Middle Ages, kings would build castles so that when their people were threatened and had to be defended, they could run inside and close the doors. From the height of the wall (the first firewall), soldiers could fight and defend the townspeople. High castle walls and the deep rivers surrounding them protected the castle. And it worked well—some of the time.

Then came the Renaissance. Far more sophisticated weapons and more organized armies demanded new defense strategies. Kings still built castles, but they understood that a castle was no longer the best way to protect the people. In fact, the opposite was true. Castles became luxurious homes for the rich; battles had to take place far away so as not to damage the castle. In the Renaissance, leaders recognized a castle was the best defense in a static world. But in an increasingly dynamic (i.e., mobile) world where everyone is a nomad, it was only a piece of the solution.

Finally, the Modern Age arrived. Today people travel around the world in planes, trains, and cars. They do global business. They rely on pieces of plastic called credit cards. They communicate with friends everywhere on the planet. Inside continents such as Europe and the Americas, borders have virtually disappeared.

Today there are no castles to protect people, but cameras and satellites are everywhere. Protection is not about the width of a wall or the size of a battlefield. It is about building an overall worldwide security system that works with individuals' behavior. This white paper will:

- **Explain** the high-level evolutions enterprises and their security officers face.
- **Point out** key considerations including people, devices, and data rating.
- **Suggest** scenarios following the information lifecycle to implement security policies in the organization.
- **Review** technologies to better secure the information technology system.
- **Discuss** the latest changes in the global environment.
- **Provide** indications, tricks, recommendations, techniques, and useful technologies.
- **Explain** how we can move from building firewalls to instilling security behaviors into each employee.

Yves Aillerie
Business Development Manager
Intel Corporation

Frank G. Gates
Solution Architect
Intel Corporation

Michel Juvin
Group Information Security Officer
Lafarge



THE EVOLVING ENTERPRISE SECURITY ENVIRONMENT

Only few years ago, during the Middle Ages of the information technology era, corporate data was moving to and from traditional PCs through wired, isolated networks to secure servers. IT organizations built castles, which they called firewalls. Information had to move within the firewalls. Security was mainly about building stronger firewalls.

Information flow has changed immensely. Now corporate data is moving to any mobile device through wireless access points to the cloud. Interaction with the data is changing at the speed of light, driven by new kinds of Internet access devices and by consumer applications and business requirements. New devices, smartphones, tablets, applications, and social media are also entering the enterprise without any security standards. Sometimes, they even break existing security standards.

We've all heard stories about senior executives of a large company meeting face-to-face and being interrupted by someone entering the room and presenting what he just collected on his PC: the contents of every smart phone in the room.

When the IT environment changes—due to employee behaviors, technologies, or geopolitical challenges—basic security requirements remain the same. The scope and efficiency of security solutions must grow for the enterprise to keep functioning efficiently.

To do this, the business must build an enterprise information security strategy that understands the business landscape and anticipates the company's evolution including changing employee needs, evolving security technologies, and the quality of new data.

When it comes to protecting the information castle—company assets like intellectual prop-

erty—the walls are the weakest point. Businesses must be highly and wisely protected. Protection must be cost effective and not slow down the company dynamic.

We are moving from an era where having knowledge is important to a new era where knowing where the information is located is equally important. This is true for both personal and corporate information.

Big players will concentrate their corporate information in databases everyone in the company can access. The goal is not only to store information safely and securely, but also to manage access to valuable intellectual property.

THE AGES OF INFORMATION TECHNOLOGY

Information technology is very young—only about a half century old. But looking back to the past 20 centuries of human history can teach us a lot about the ages of security:

- **The Garden of Eden.** Everyone was playing nicely. Computer security was unheard of and unnecessary.
- **The Age of Mischief.** Attacking a network was a challenge to individuals, but there was little or no malicious intent. It was for advancing one's reputation with other attackers. There was some concern about data being erased or modified.
- **The Age of Individual Reward.** Altering or copying data on computer systems was for personal gain or anonymous malicious intent.
- **Organized Crime.** Attacks are authored and prosecuted by organizations, typically to steal data and hold it hostage or resell it. Individuals are consumed by larger organizations.

THE VALUE OF INFORMATION

The market value of a company has changed since the 1900s, when it was based on production investments such as railways and factories. In the 1950s, market value was mainly based on buildings and land. In the 21st century, companies with the highest and fastest-growing value are the ones with the greatest information capital. These are companies like Google or Facebook that are at the center of the digital economy. This trend is growing exponentially: According to IDC, 1.8 zettabytes of data (1800 BGb) were created in the world in 2011 (Figure 1).

Another challenge that may arise is differing memory configurations. Here things get a bit more complex; however, we can assume the memory increase is also part of evolution, and that memory differences in the same timeframe are due to the fact that increasing memory would have given little or no benefit but would increase the overall cost.

We should consider our information heritage and protect it based on our culture and organization. One suggestion is for companies to include a paragraph in their annual reports on how they manage their information capital and keep it safe from hackers.

BREAKING DOWN BORDERS

In geopolitical terms, keeping a country secure has always meant building strong border defenses to detect undesirable individuals or goods and deny them entry. Thus, immigration and customs services were born. Then, as now, they were given great powers to act decisively in the moment.

Until recently, information security was very similar. It meant dividing the world into “us” and “them” and investing heavily in strong defenses to prevent movement between the two regions. These domains became public and private networks, and firewalls handled security. As with the real-world security organs, the firewalls were granted great powers which could absolutely prevent certain data from passing. Often, this was to the inconvenience of users. But even as firewall technology evolved, this inconvenience was deemed acceptable.

Fast-forward to today. There are at least two significant developments in keeping countries safe:

- **Borders** have been made less complex or even removed so that people can move freely between participating nation-states.

- **The possible repercussions** of people moving or moving certain goods have become overwhelmingly severe.

Recognizing that it has become untenable to police their borders, many nations are switching their investments into intelligence services and technologies that work to detect intent and better identify the real threats among the expanding number of non-threats.

This shift toward open borders and intelligence gathering is also mirrored in the networking world. Network borders are becoming more numerous (e.g., every USB port, every mobile device, and every poorly supervised network protocol). At the same time, users are demanding more flexibility to accommodate an impossibly large number of critical applications and communication needs. Firewalls, while still an essential part of a security strategy, cannot be the whole strategy. Instead, a number of specialized network infrastructure appliances are evolving from the earlier intrusion detection and later intrusion prevention appliances. These new security appliances must be positioned within the protected network to detect and suppress threats between subnets. Security has become a matter of detection, heuristic learning algorithms, and agile suppression—not inflexible pass and block configurations.

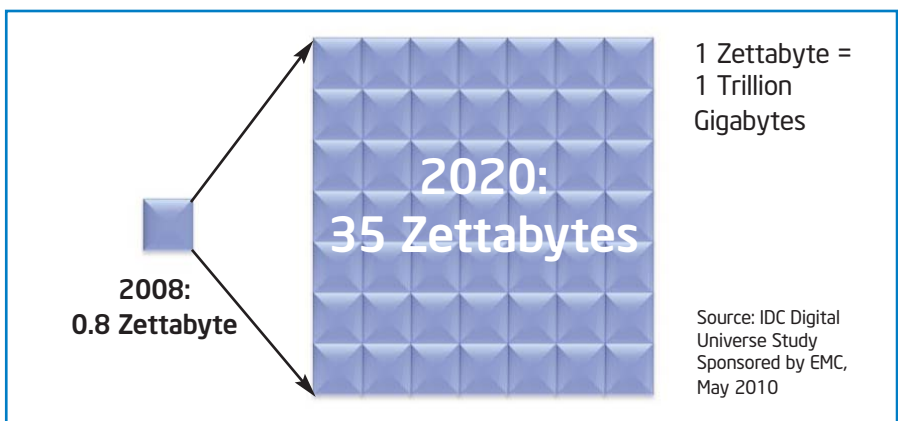


Figure 1. The Digital Universe, 2008 to 2020

Better Security Drives Innovation

Just as nations can best defend against global threats by having their intelligence organizations collaborate with others and always attempting to discover new correlations of behavior that signal intent, network security must increasingly rely on collaboration between security devices—even between data networks operated by diverse users. In the recent past, this was done informally by security vendors sharing information on new threats as they attempted to seize market share by demonstrating advanced competence in defeating all threats.

Today, autonomous alerts come from probes located within appliances. They communicate unusual behavior to a central organization, which may exist within the protected network or be shared between networks. The central organization determines whether the threat is real and, if it is, how to defend against it. The response is then distributed to the front-line appliances to eliminate, suppress, or contain the threat.

To quote Juvenal, “Who will guard the guards themselves?” This has been the difficulty with every security organization and every data network. If one element is corrupted, can you trust any? Best practice is to establish the trust of a few individuals or elements and derive trust from those elements while enforcing a need-to-know policy designed to limit the effects of any failures. In data security, this means using a public key infrastructure and a mechanism to maintain security certificates. Again, this has triggered a new species of network security element with a very specialized role, yet which must be granted the ultimate trust. No matter how trust is centralized and concentrated, it is crucial that the core object of trust be protected, authenticated, and tamper-proof/tamper-evident.

Today, security is about who you are. Can we trust you? Do we know what you might do in the future? This is more important than what you are trying to do right now. Zero-day attacks are inevitable in an open society. Similar to lone-wolf terror attacks, they demand fast responses and indications of intent to defeat them. Heavily policed societies are now unacceptable and stifle progress. Today’s security solutions are autonomous defenses such as intrusion prevention instead of intrusion detection and manual firewall configuration.

Table 1 shows some of the key threats in today’s security environment.

The greatest challenge is protecting the foundations of society without interfering with its day-to-day functioning. Solutions come at a price—in both performance and capital—but are worth it when they can help avert a catastrophe.

MEET GENERATION Y

A decade ago, users were comfortable working from a fixed location with a single platform and a wired phone. But over the last

five years, Generation Y—born between 1975 and 1995—arrived in the workplace. These employees have a very different mindset than older-generation employees. They bring new devices that are lighter and smaller than traditional workstations and laptops. They also bring opportunities to multi-task and connect to several end points. These employees grew up with mobility and belong to a social network that knows no boundaries. Along with these new technologies and products, Generation Y also brings new workplace behaviors.

Never before has a generation had so much influence on the existing workforce. The industry generated this influence by competing to continually innovate. But this same industry does not fully understand the scope of this evolution and its impact.

The new generation of employees not only brings personal solutions into professional domain (i.e., consumerization), they also bring a completely different view of what information means. Enterprises need to learn from them. At the same time, the company needs to teach senior employees how to differentiate among the many types of

Table 1. Security Breaches Caught

31,000 new phishing incidents per month (<i>McAfee</i>)
11 million U.S. victims of identity theft in 2011 (<i>Javelin Strategy and Research</i>)
1.5 million Facebook* IDs for sale in 2010 (<i>ABC News</i>)
30,000 Gmail* and Yahoo* passwords posted online (<i>Daily Mail News</i>)
81 percent of consumers consider phishing a significant concern (<i>ITRC Survey</i>)
54 percent of companies had a data breach in 2010 (<i>Forrester Research</i>)
88 percent of Fortune* 500 companies affected by Zeus* (<i>CNET Survey</i>)

information and interact with it. Today's users demand multiple platforms and interfaces, from laptops to smartphones and tablets.

To put it in sociology terms, Gen Y employees are like a nomadic tribe. And from an enterprise standpoint, a tribe is a security challenge. In medieval times, inside the castle, a tribe would have guilds of people doing similar jobs. Back then, these guilds were easier to control. Why? Simply because they were less numerous and they worked in a limited territory—mostly inside the castle walls.

Gen Y employees are also connected to communities such as sports teams and groups of friends. Each group is a tribe, and each person can be virtually connected to several tribes. Each tribe has its own (usually unwritten) laws that are nothing like the organization and structure of a company. So today there's a disruption between the external world and the enterprise—and key influencers might be outside the typical hierarchy. This also means that young employees might create expert communities with their own rules.

Whether organizations like it or not, Gen Y employees carry their communities with them—which is sometimes for the best. Working with their tribes can generate more value for the company than a single employee could generate working alone. The company shouldn't refuse this added value, but needs to look for the best employees working with the best tribes.

To adapt to these changes Intel, for example, has very few restrictions for employees using company PCs. Employees can have personal data stored on their company laptops. This means an employee's information access device might be the same for both their private and professional lives—which must be considered from a security standpoint. The latest trend is to bring your own network (BYON). This shows the impact the network has on each one of us as the distinction between personal and professional worlds becomes increasingly fuzzy.

For example, one company offered each employee free Internet access. Employees were able to create their personal links and communities both inside and outside the enterprise. On specific technical topics, employees opened up discussions to the external world, where they found experts, solved outstanding issues, and even discovered unexpected opportunities. Everyone from top management to the cleaning staff started to complement their daily jobs with connections to the external world.

Of course, opening up the corporate network poses security and organizational issues. Management's role is changing, since the manager is no longer the center of knowledge. Instead, knowledge is shared within communities. The manager's role is to anticipate, organize, and facilitate. If the company does this well, it can produce innovative product lines and better position itself for success. By providing additional freedom to employees, the company lets them find their own ways to create value for the company.

At the same time, IT systems must be secured to protect the company from danger. Security must be embedded in the information system in a way that lets employees still feel free to generate value.

INFORMATION STORAGE

Protecting data has three key components:

1. **Data at rest:** Protecting the data where it is stored
2. **Data in motion:** Protecting data while it is being moved or transported
3. **Data processing:** Protecting data while it is being used

Any data security solution must consider all three, since data is only as secure as its most vulnerable mode.

The modern way to secure data at rest is encryption, which attempts to reduce or erase

the value of stolen data by temporarily transforming it to make it useless to anyone but the rightful owner. Decrypting the data requires keys, which are small enough to be easily protected.

Data in motion doesn't actually move; it is copied from place to place until being delivered to its destination. All those copies become a data security problem unless they are of no value. Once again, encryption is the preferred solution. If data is encrypted, then the owner is unconcerned about how many copies are made or who has them. There are well-known ways to protect the encryption keys.

Data processing is the third problem. Data has no value unless it is used. To be useable, it must be unencrypted and in a data processing machine. Any data processing machine will pass data over various buses, hold it in memory, and manipulate it in sight of many other processes. Making the data secure while it is being processed requires shrinking the size of the logical machine to reduce the number of elements that must be considered and ensuring that data held outside this core of trusted elements is protected as if it were at rest or in motion. In this way, you can limit data's exposure to outside attack to a logical and physical location so small that it may only exist within a single silicon die, with physical features that preclude tampering.

Moving from a predefined location, where data is kept under strict and internal surveillance, the information is now inside and outside the walls, with different monitoring. As we explained, this move was due to the size and opportunity of exchanging beyond company infrastructure and walls.

Valuable information is created by associating different types of content. This opens the door to risks and vulnerability. For example, Lafarge—a French company specializing in cement, concrete, aggregates, and gypsum—needs to share information between

its core infrastructure and contractors. The information requires different levels of controls, which are handled by either the Lafarge infrastructure or by Lafarge's suppliers. Lafarge's engineers develop ideas using their own networks, which are outside the company wall. They create high-value information by merging information from both inside and outside the wall. This high-value information becomes innovation, which makes it a target for hackers.

In the recent past, creating and selling a simple object was easy enough. Let's take a glass as an example. Based on design, artwork, and raw material, any company could easily create and bring to market a glass. Nowadays, to deliver a new product, a company must:

- **Trace** the history of the raw materials that go into the product
- **Design** the product to specific market niches and packaging constraints
- **Ensure** the product complies with local, national, and sometimes international regulations
- **Tag** the product
- **Ready** the product for alternative sales channels including online

This complexity will increase in the future, with more and more complex systems using more data to generate even more data. Technology can help make it affordable to manage this data explosion, with systems that help a company visualize, use, and analyze the data.

ABOUT INFORMATION: PERFECTLY OR PARTIALLY TRUE?

Over the last 10 years, a new reality has emerged: the perfect, undisputed truth of a piece of information.

Consider search engines. When a user launches a search query, it is important for the search engine to provide a great deal of information in a fraction of second, even if only the first 10 pieces of information make sense or the information does not reflect a scientific reality. In this case, the number of hits the search engine returns is information in itself, showing a trend, which is a kind of truth.

Another example is weather forecasting. We will trust weather forecasts as far as 10 days out. Is this information true? No. And we know this information is not something we can fully trust. Still, we want this information and we want more of this kind of information.

Today, we take for granted any piece of information. The cost and effort to obtain it don't scare us, so we don't mind being drowned in a sea of information. How do we handle this information? Should we go further to find out if the information is 100 percent accurate? The answers depend on our needs and our interest in a certain situation. We should find a strong filter and count on a security model that helps us find the right piece of information and use it correctly.

BUILDING A STRATEGY

Understanding the Renaissance

Let's go back to the Middle Ages and castles. Do we really know why they disappeared? Was it just because soldiers invented more sophisticated weapons?

Guns appeared at the end of the 14th century and even larger walls could not protect people against these new tools of attack. But this is only part of the story. Cities were protected with walls up to the 17th century, and bunkers were still built in the very recent past.

So what replaced the castles and the fortresses? From the Renaissance to today, security has progressed, and that progression is still underway. Some highlights:

- **There are new** and more sophisticated classes of weapons.
- **Technologies and processes** aim to better protect individuals—for example, security cameras and check-in at airports.
- **New global political and philosophical systems** are in place and still progressing. The Renaissance brought humanism, more consideration for human life. Democracy has tried to improve individuals' lives; create constitutions, rules and laws; and educate the masses. These are certainly highly efficient security ingredients.
- **Security** is a complex system, combining many interacting factors.
- **We need to protect ourselves** and others; however, security is a never-ending war. There's no permanent protection solution that is 100 percent safe. We need to understand this and implement a security philosophy and process to help track, implement, and secure information as much as we can.

Role of the CISO

Once, an enterprise's chief information security officer (CISO) was like a local police officer. Today, the CISO is more like the state security apparatus.

The CISO's first job is to bring security into the enterprise. But often, employees see security as a few individuals painfully slowing down the work of the enterprise.

At Intel, for example, every employee is trained every year on security awareness at

a mandatory yearly meeting. Every employee is made aware of risks, educated on behaviors, and made to understand the challenges. In short, every employee is a security agent.

Another important role of the CISO is to understand the global picture—that is, the security picture beyond the specific business of the enterprise. This includes geopolitical trends.

The CISO also needs to understand information flow, including where it comes from and where it goes, as well as the value of information to the company.

Finally, the CISO needs to develop a long-term security strategy that is approved by company management. That strategy needs to include:

- **Implementing ethics and ethical rules in the enterprise.** Everyone must behave with both professional and personal ethics. Ethics must be part of the enterprise's key values.
- **Creating security governance.** Everyone must be aware of the risks of sharing information over the public network. It is not the CISO's responsibility to evaluate the cost of the information exchanged, but he must have enough basic knowledge to give the right advice.

In some cases, the CISO is considered a risk manager simply because it is in his role to analyze the opportunities, costs, and risks of activities that are essential to each employee's job. To train and educate users, CISOs should have the support of the HR and legal departments.

Classifying Information

Security is about who can access what kinds of information and how. Each piece of infor-

mation has a degree of confidentiality, availability, and integrity. All of the company's information must be rated for these three factors. The knowledge manager implements this assessment process.

This is especially important for the organization's most critical, highly confidential information, which must be clearly identified and made accessible only to authorized employees. The knowledge manager must be in synch with company executives and have enough power to ensure that strict rules are enforced.

In short, the information manager's role is to classify all company information and build a security process and strategies around each class. Understanding the information cycle is basic to implementing this process.

INFORMATION MANAGEMENT

About Information

Companies have one mission: creating value. A company creates value for employees, shareholders, and customers. Value is a complex concept with multiple ingredients. One of these ingredients is information, one of the company's most strategic assets.

Information is under attack and must be protected. Understanding how information flows makes it clear where and when it is most vulnerable. It is essential to consider the evolution of information, from creation to storage, to understand which data should be protected and when it is most vulnerable.

Data versus Information

Data has no value without context. For example, the number 50,000 is a piece of data, but it has no meaning unless you know that EUR 50,000 is the annual salary of Mr. Smith. Data with a specific context becomes a piece of information.

The Information Lifecycle

The information lifecycle has four steps:

1. Creation
2. Classification
3. Materialization
4. Enrichment

From CISO's standpoint, there are two main flows for data creation (Figure 2):

1. **Information generation by employees.** Engineers, or any employees, develop new information by exchanging ideas with colleagues internally. They might also get information from outside the walls of the enterprise. This starts the process of data creation.
2. **Information generated inside a predefined process** (most of the time within an enterprise resource planning solution). Data are created and materialized automatically.

As soon as information is created, its level of sensitivity must be assessed so that it gets the right level of protection. According to the International Organization for Standardization (ISO) International Engineering Consortium (IEC) 27002 information security management code of practice, "Information should be classified in terms of its value, legal requirements, and level of sensitivity and criticality to the organization."

The sensitivity level of the information corresponds to the information's confidentiality objectives (Figure 3). Information is protected against damage caused by disclosure through appropriate handling procedures.

The criticality level of the information corresponds to the information's integrity and availability objectives. This involves protecting

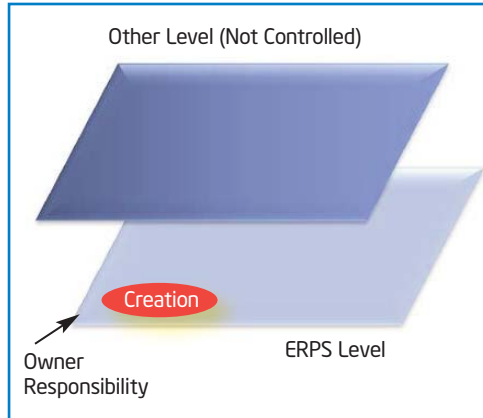


Figure 2. Understanding the Information Lifecycle

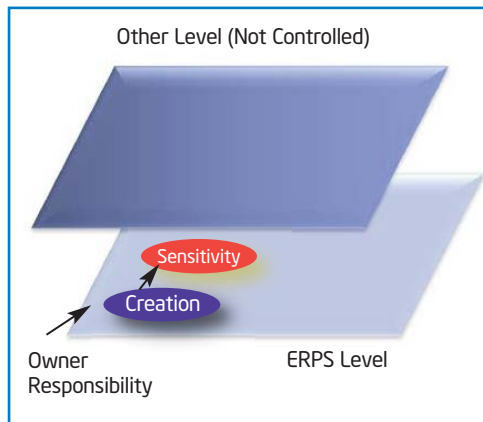


Figure 3. Information Sensitivity

the information against modification and destruction through appropriate handling procedures, which are distinct from the sensitivity procedures.

The next step is materialization (Figure 4). After creators have a new and valuable idea, they materialize the information electronically on a server or computer. Data must be classified before materialization can begin. Classification defines the availability level, integrity, and confidentiality requirements of the information (Table 2).

Following a workflow mainly defined by its sensitivity level, the data receives input from a user or event. This enriches the data, adding value (Figure 5).

The workflow defines a protected environment. It means that if data is extracted from the workflow, it increases the risk of hacking. Users sometimes need this extraction to improve their efficiency or control. Regardless, it exposes the data to vulnerabilities which are difficult to identify.

For example, if the originator of an idea or prototype presents it to a community, the idea can be enriched with input from the community members. Still, this presentation to the community must be carefully managed, depending on the sensitivity of the data.

The next step is the deliverables. At the end of the workflow, the data is stored in a database with protected rules defined by user access rights—until someone links this data to others to recreate other valuable data, which will get into the same lifecycle (Figure 6).

Data vulnerability to hackers extends from materialization until the end of the cycle. IT must find a solution for protecting the information during this vulnerable period. Several solutions can be identified, but policies and standards can decrease the risk by:

Table 2. Information Classification			
Information Security Objectives (CIA Triad)	Protect Against Damage	Classification	Classification Level
Confidentiality	Disclosure	Sensitivity	<ul style="list-style-type: none"> ▪ Public ▪ Internal use ▪ Confidential ▪ Highly confidential
Integrity	Modification	Criticality	<ul style="list-style-type: none"> ▪ Minimum ▪ Medium ▪ Maximum
Availability	Destruction		

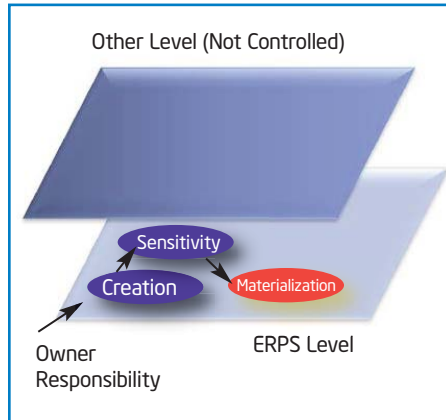


Figure 4. Materialization

- **Classifying the data** by level of confidentiality, accessibility, and availability,
- **Defining a tool** for encrypting data, depending on how it is managed.

SOLUTIONS

Trust

The model in Figure 7 approaches trust as a factor of two feedback loops. The half-circle on the left represents the processes needed to generate trust. The half-circle on the right represents processes that have the potential to destroy trust.

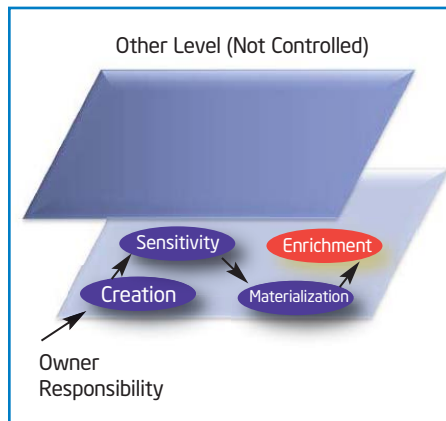


Figure 5. Business Workflow Enrichment

If you approach trust (security) from a purely technical perspective, as a factor primarily of remedies and infrastructure, you never establish a trusted relationship with your business. While this may be adequate for a closed security system (i.e., one group driving security for an enterprise with no questions asked), it simply will not work when you expand into a cloud community. Again, there are significant security cost implications if you do not establish trust through the broader cloud ecosystem.

Security Components

As we discussed earlier, one key ingredient of the new security landscape is education of employees with executive sponsorship. To train and educate users, CISOs should have support from the HR and legal departments, especially in companies having intellectual property and/or trade secrets. This must include regular updates for ongoing security education.

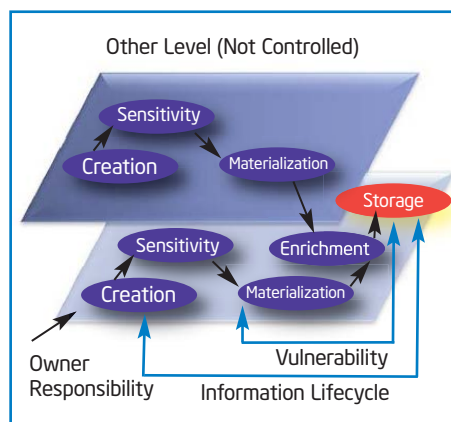


Figure 6. Business Activity on Different Mobile Platforms

Security Process

The security process starts with identity and access management (IAM). This means each sensitive document must include the author's name, verification of the author's name, and

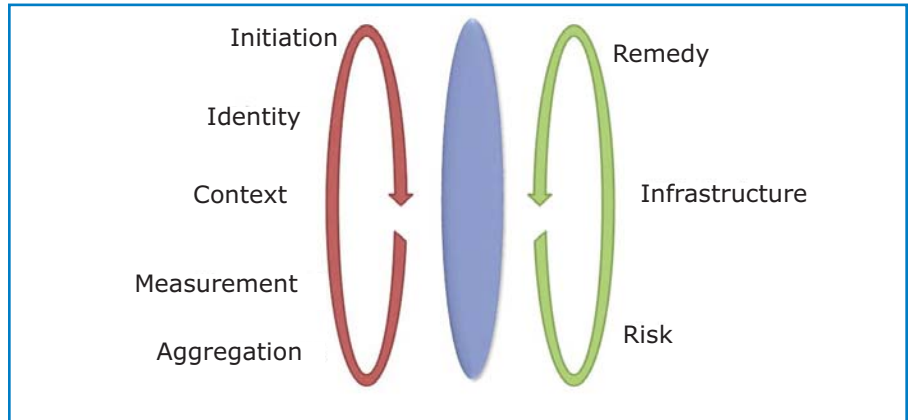


Figure 7. Trust Model

the level of authentication. It ensures that the right person has the right information access (e.g., “You are an accountant; your role is...”).

This is not easy to implement or maintain. For example, password management on sensitive documents may seem simple, but what happens when the authorized employee is away?

IAM requires you to think thoroughly about your organization and to map your sensitive information to match it. If a company hasn’t implemented an IAM procedure, newcomers will generally receive access to shared drives and other data storage locations from the assistant to the department head. Users receive access rights from a business process owner who delegates this role to one member of each team.

This process generally works well, but makes it hard for the company to have a consolidated view of all of its data.

For example, in a large airplane manufacturing company, designing and implementing a security policy can take several years, with dozens of highly qualified people involved. The resulting strategy, however, can be used for several decades.

Technical Implementation

One good practice is to link the data to its “reputation,” encrypted information defined by the workflow and the type of access to the information (e.g., read, copy, send, archive, and print). This involves:

- **Read mode:** Following a regular process, a user asks to retrieve information. At the same time, he automatically ensures the pedigree of the information any time it is copied.
- **Updating information:** After receiving read access to the information, the user updates it, along with the information’s reputation.

- **Copying or sending information to another digital support:** There are two ways to copy information: the simpler way, without a reputation, and the more secure way, with a reputation.
- **Stolen information:** When data is lost, it's possible to double-check the reputation and verify the workflow and pedigree of the information. This means the reputation must be automatically encrypted and closely linked to the data. It is best to access the reputation from inside the chipset.

INTEL AND SECURITY

Throughout its history, Intel has pushed the boundaries of what's possible to improve how people live and work. Intel's vision is defined by three powerful pillars:

1. Energy-efficient computing
2. Connectivity
3. Security

Intel bases its strategy on delivering high-quality products, providing strong service solutions, cultivating a rich ecosystem, and striving for innovation. Intel is focused on delivering solutions to end users to help them benefit from a quality, consistent experience across all devices.

Different Intel technologies are aimed at detecting and protecting from malware, recovering and enhancing patching, protecting identity and deterring fraud, and securing data and assets (Table 3).

Intel® Identity Protection Technology (Intel® IPT)

As identity thieves become more advanced in their hacking techniques, Intel has built two-factor authentication directly into the processors of select 2nd generation Intel® Core™ processor-based PCs, helping to prevent unauthorized access to important personal accounts. Two-factor authentication is the standard in identity protection technology. Using one factor, something you know (like a username and password) and adding another factor, something you have (in the case of Intel IPT, a six-digit, one-time password linked to your PC), two-factor authentication improves your level of security. With Intel IPT, this unique one-time password (OTP) changes every 30 seconds, so even if thieves are able to obtain your username or password, the code is difficult for thieves to predict.

Intel® Expressway Cloud Access 360 (Intel® ECA 360)

Cloud adoption has been slow due to overwhelming security complexity and the lack

of comprehensive solutions that can effectively project an enterprise-class security model on the cloud. Today, users have set up redundant accounts with weak passwords that are disconnected from the corporate identity infrastructure, user actions in software as a service (SaaS) apps have no oversight or authorization—leading to sensitive data leakage and compliance risks, and lack of standardized logs block administrators from monitoring or correlating cloud user activity with internal audit repositories.

So how does the enterprise regain control in an environment where security models change by cloud provider or are left entirely up to the enterprise? Intel® Expressway Cloud Access 360 software is the first solution suite designed to control the entire life-cycle of cloud access security, providing SSO, provisioning, strong authorization, and audit. Capabilities include:

- **Control.** Account de-provisioning, identity data synchronization, fine-grain AuthZ.
- **Visibility.** Monitor API access activity, SLA alerts, central admin console.
- **Compliance.** Auth soft/hard OTP, log correlation to audit repositories, de-provisioning.

Table 3. Intel Security Technologies

	Identity Protection and Fraud Deterrence		Detection and Prevention of Malware		Securing Data and Assets			Recovery/Enhanced Patching
	Intel® Identity Protection Technology (Intel® IPT)	Intel® Expressway Cloud Access 360 (Intel® ECA 360)	Intel® Virtualization Technology (Intel® VT)	Intel® Trusted Execution Technology (Intel® TXT)	Intel® Anti-Theft Technology (Intel® AT)	Intel® Insider™	Intel® AES-NI	Intel® vPro™ Technology
PC	✓		✓	✓	✓			
Server		✓	✓	✓		✓	✓	✓

Intel® Virtualization Technology (Intel® VT)

Intel® Virtualization Technology (Intel® VT) is a set of silicon-based features available from Intel® server, desktop, and mobile processors that complement software-based virtualization technologies to add greater manageability, security, and hardware utilization to the enterprise.

Intel® Trusted Execution Technology (Intel® TXT)

Intel® Trusted Execution Technology (Intel® TXT) provides hardware-based security technologies to build a solid foundation for security. Built into Intel's silicon, these technologies address the increasing and evolving security threats across physical and virtual infrastructure by complementing runtime protections such as anti-virus software. Intel TXT also can play a role in meeting government and industry regulations and data protection standards by providing a hardware-based method of verification useful in compliance efforts.

Intel® Anti-Theft Technology (Intel® AT)

Fact: A laptop is stolen every 53 seconds, while 12,000 laptops disappear every week from U.S. airports alone. Of all lost laptops, 46 percent had confidential data and no encryption.

Giving users access to corporate data and applications through remote laptops boosts productivity, but misplaced laptops can leave IT vulnerable to hackers. Intel® Anti-Theft Technology (Intel® AT) is built into laptop hardware, helping IT administrators outwit thieves, even when they attempt to reimage the OS, change the boot order, or install a new hard drive.

When laptops with Intel AT become lost or stolen, they can be remotely disabled. If the

laptop is recovered, it can be quickly reactivated to normal operation.

Intel AT is available on select 2nd generation Intel® Core™ and 2nd generation Intel® Core™ vPro™ processor family-based laptops when activated with a service subscription from an Intel AT-enabled service.

Intel® Insider™

Intel® Insider™ is a feature that enables consumers to enjoy premium Hollywood feature films streamed to their PCs in high-quality 1,080p high definition. This service has not existed in the past because the movie studios were concerned about protecting their content and making sure it cannot be stolen or used illegally. Intel created Intel insider as an extra layer of content protection. Think of it as an armored truck carrying the movie from the Internet to the display. It keeps the data safe from pirates but still lets the user enjoy legally-acquired movies in the best possible quality. Built into the latest Intel processors, this technology will become even more important once wireless display technology becomes more popular, since it would prevent pirates from stealing movies remotely.

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government in 2001. It is widely used across the software ecosystem to protect network traffic, personal data, and corporate IT infrastructure. AES is a symmetric block cipher that encrypts/decrypts data through several rounds.

The Intel Core processor family includes a set of new instructions, Intel® Advanced Encryption Standard New Instructions (Intel®

AES-NI) that helps to implement some of the complex and performance-intensive steps of the AES algorithm using hardware, thus accelerating the execution of the AES algorithms. AES-NI can be used to accelerate the performance of an implementation of AES by three to 10 times over a completely software-based implementation.

Intel® vPro™ Technology

Managing and protecting desktops and laptops and securing data are among the great challenges for modern businesses. The 2nd generation Intel Core vPro processor family with the hardware-based security and manageability of Intel vPro technology simplifies and accelerates these critical IT functions.

Intel vPro technology is a set of security and manageability capabilities built into the 2nd generation Intel Core vPro processor family, Intel® chipsets, and network adapters.

With security and management features built into the hardware, Intel vPro technology:

- **Accelerates data encryption/decryption** using Intel AES-NI, improving user productivity.
- **Significantly reduces** unwanted access to sensitive data on missing laptops using Intel® Anti-Theft Technology.
- **Enables IT technicians** to quickly deploy security patches across PCs, remotely unlock encrypted drives, and manage data security settings
- **Gives IT help desk** personnel complete control over a PC with features like KVM Remote Control.
- **Enables IT** to remotely troubleshoot and repair PCs.

SECURITY INITIATIVES

Intel's upcoming security initiatives include:

- Next-generation end-point security
- Secure embedded device security
- Secure mobile device security
- Cloud security platform

As Intel has elevated the priority of security to be on par with its strategic focus areas in energy-efficient performance and Internet connectivity, its future initiatives concern the next-generation end-point security, a cloud security platform, and the security of embedded and mobile devices.

CONCLUSIONS

Whatever the environment, a CISO must continually help the company take advantage of the benefits of using information. This includes information moving both inside and in and out of the company. The best CISO is the one securing the highest level of security while allowing the most efficient information system, while keeping his company open to outside value. This involves being able to:

- **Understand.** The CISO must understand that information is a valuable company asset, no matter what the format.
- **Anticipate.** The CISO needs to anticipate hackers by understanding the global worldwide environment and geopolitical effects of information and anticipate changes in the way employees interact with information. It is important to implement an information "war" strategy.
- **Educate.** The CISO must educate both employees and company leadership so that everyone understands the importance of information security and how to maintain it.
- **Implement.** The CISO must find the right security technologies and systematically assess the company's overall security system. It's essential to constantly assess and implement new technologies.
- **Maintain.** Finally, even today's open enterprise is still like the castle of the Middle Ages. IT still needs high castle walls in the form of highly reliable firewalls.



About Intel

Intel (NASDAQ: INTC) is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world's computing devices. Learn more at www.intel.com/itcenter.

About Lafarge

Lafarge is the world leader in building materials, with top-ranking positions in all of its businesses: cement, aggregates and concrete, and gypsum. With 76,000 employees in 78 countries, Lafarge posted sales of EUR 16.2 billion in 2010. Learn more at www.lafarge.com.

Find the solution that's right for your organization. Contact your Intel representative, visit Intel's Business Success Stories for IT Managers (www.intel.com/itcase-studies), or explore the Intel.com IT Center (www.intel.com/itcenter).

ABOUT THE AUTHORS

Yves Aillerie joined Intel almost 20 years ago and has had many roles, mainly in sales and marketing, in both France and Ireland. He is currently a business development manager based in France, dedicated to the energy market segment. In recent years he has focused on making energy personal, working in open innovation mode with industry and academic collaborators to build solutions for reducing electricity consumption in buildings.

Frank Gates has worked with network security and related technologies for over 20 years. His experience in telecom and network engineering R&D led to 10 years as a platform solutions architect at Intel, focusing on the needs of the embedded Intel® architecture opportunities in network security and other network appliances. In 2011, he joined Intel's Sales and Marketing Group as a solutions architect, again bringing his network security knowledge to bear.

Michel Juvin is group information security officer at Lafarge, reporting to the CTO and VP internal controller. Michel joined Lafarge in 1999 as an internal IT auditor, developing the IT internal audit team, devising the IT internal audit guide, and leading about 20 IT missions worldwide. Afterwards, Michel was appointed CIO for the cement subsidiary in France, leading a team of more than 35 IT specialists and covering both industrial and office information systems. Michel then moved back to a more functional role, leading information security and IT internal control for the group. He was responsible for defining information security policy and standards and helps BU IT managers to define their internal control reports on a timely basis.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit Intel Performance Benchmark Limitations.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information. The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

Intel® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. For more information, see <http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/>.

Intel® vPro™ technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: <http://www.intel.com/technology/vpro>.

No system can provide absolute security under all conditions. Intel® Anti-Theft Technology requires an enabled chipset, BIOS, firmware and software, and a subscription with a capable service provider. Consult your system manufacturer and service provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit <http://www.intel.com/go/anti-theft>.

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit <http://www.intel.com/technology/security>.

Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit <http://www.intel.com/go/virtualization>.

Intel® Insider™ is a hardware-based content protection mechanism. Requires a 2nd gen Intel® Core™ Processor-based PC with built-in visuals enabled, an internet connection, and content purchase or rental from qualified providers. Consult your PC manufacturer. For more information, visit www.intel.com/go/intelinsider.

No system can provide absolute security under all conditions. Intel® Identity Protection Technology requires an Intel Identity Protection Technology-enabled system, including a 2nd gen Intel® Core™ processor enabled chipset, firmware and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit <http://ipt.intel.com>.

Copyright © 2012 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

Joint consideration from Lafarge and Intel

*Other names and brands may be claimed as the property of others. Printed in USA SS/FG/0112/PDF Please Recycle

