Guarding what's really valuable

Information Security over Infrastructure Security

brainloop

The information security threat landscape

Securing your information has never been more important. With the continued rise of cybercrime and the increase in incidents of data loss, organisations are under more pressure than ever before to ensure that their assets are effectively protected.

Identifying the challenge is simple, but overcoming it can be difficult.

Many organisations are investing in improving security – PWC recorded a 51% increase since 2012, and yet, the number of breaches reported continues to rise.

Finding an effective, comprehensive security strategy requires more than bigger, stronger padlocks and firewalls protecting a company's perimeter.

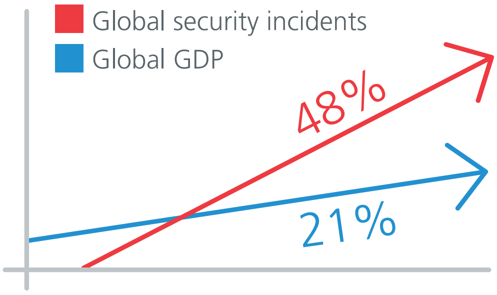
The greatest source of all security breaches over the last year was employees and former employees. This suggests that securing applications and systems is only part of the solution. Businesses need a change of mindset to better protect their valuable information, without forcing harsh security policies or unworkable processes onto employees and partners.

Let's consider how organisations have traditionally approached security – by protecting their infrastructure.

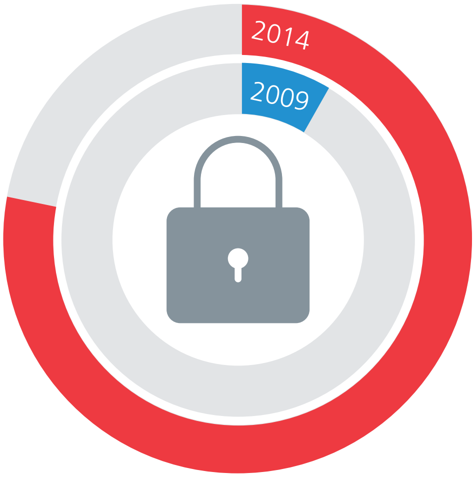
<<Europe reported a 41% jump in the number of cybercrime incidents detected over 2013.>>

The Global State of Information Security Survey 2015, PWC

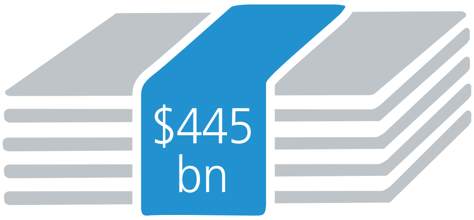
Figure 1: Information security landscape



Amount of security incidents



Global cost of cybercrime



Sources:
i - The Global State of Information Security® Survey 2015, PwC
ii - The Global State of Information Security® Survey 2015, PwC
iii - Net Losses: Estimating the Global Cost of Cybercrime, McAfee, July 2014

Infrastructure security has limitations

For many CIOs and CISOs, the instinctive start point for security is to protect physical hardware and systems from malware, viruses and a host of other cyberthreats. Then they protect the applications and data that run on those systems and support everyday operations for 'business as usual'.

Protecting the vast quantities of data that every organisation generates is unquestioned as a necessary pillar of achieving security. But how valuable really is this data? Of course, customer records, financial transactions, credit card details are the kind of data you don't want to be compromised. These bodies of data tend to exist in database applications that can be wrapped in layers of security technologies – the data itself however remains vulnerable to leakages as soon as it is transferred or exported from the secured application.

And what about the hugely valuable information found in everyday documents? Reports, forecasts, presentations, plans, proposals and personal data are often overlooked in securing what's valuable to the business and necessary for compliance.

Even more: Despite the focus on securing the infrastructure where data is housed, the raw data often has little worth in and of itself. Only when it is analysed, interpreted and converted into intelligence can it truly be considered valuable. Data is simply the raw material that is used to create the end product; the ore that is processed to create the gold bar.

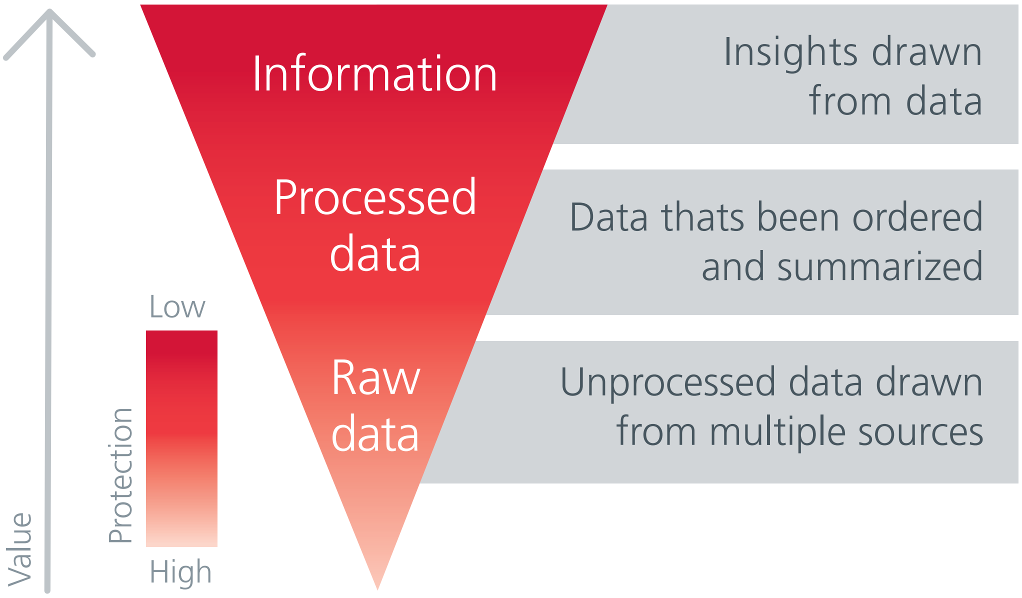
The intelligence extracted from this raw data however is rarely stored on one secure system that can be tightly locked down.

Company insights are the preserve of employees; often shared through email, cut and pasted into disparate pieces, usually filed in multiple locations – it's this highly valuable information that often resides in an unstructured, unprotected and unencrypted format.

Security decision-makers need to address effective security not only for infrastructure, but also for information.

> *<<You may have the cleanest network in the world, but you will want to talk to other people who don't. As soon as you do, you put yourself at risk.>>*
>
> *Andrew France, CEO, Darktrace and former deputy director, GCHQ*

Figure 2: Title: Value vs protection of data and information


Information
Insights drawn from data
Processed data
Data thats been ordered and summarized
Raw data
Unprocessed data drawn from multiple sources
Low
Protection
High
Value

Valuable intelligence leaves your organisation every day, unprotected

Every day organisations share valuable data with customers, suppliers and partners and they in turn share it with others. This information ends up stored on a range of insecure devices, such as smartphones, tablets, laptops and USB sticks.

Even in rare cases, where an organisation limits the circulation of intelligence or filesharing to its internal users, guarding against employees distributing the data beyond the reach of security teams is still a challenge.

According to TrendLabs, 56% of employees frequently store sensitive data on their laptops, smartphones, tablets and other mobile devices. What's worse is that the data on these devices is typically unguarded; in fact 65% of SMBs report that their organisations' sensitive or confidential business information is not encrypted.

Valuable, or even sensitive information, will leave the walls of your organisation – whether unintentionally or maliciously.

It is likely that employees going about their daily business will simply distribute the intelligence you have spent a significant amount of time and effort protecting from external attacks, to external parties.

The expensive firewall, the encrypted fibre network, intrusion alarms and malware detectors will all be rendered ineffective - the equivalent of building Fort Knox and leaving the keys in the door.

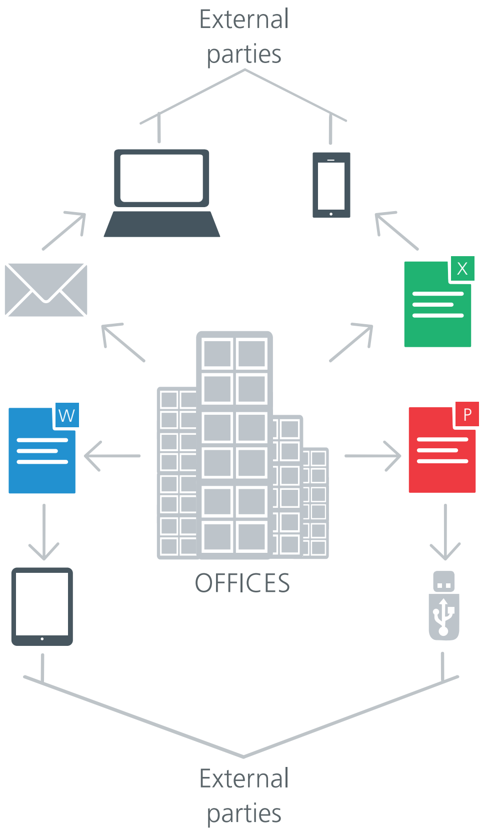
So how can CIOs and CISOs find a way for users to take responsibility for the security of the information they handle? Or should the company aim to control the way users behave?

With the first scenario, achieving a mass shift in culture is a lengthy and high-risk strategy to count on. Applying complex security policies, or expecting users to comprehend encryption is too onerous and they will find a workaround. On the other hand, leaving security policy too open could create more problems than it solves. We need another way.

<< I see the insider threat looming larger in my windshield than in my past. Insider threats are not always a 'bad guy' with bad intentions, it could be a good employee doing righteous work in an insecure manner. Our problems are more human than technological.>>

Michael A. Mason, Chief Security Officer, Verizon Communications

Figure 3: Where your information ends up



The problem with policy

Information security policies are all too often written from a theoretical, rather than pragmatic, point of view. Produced by technical teams, they are commonly packed with complex jargon covering every bit and byte, and written with no consideration for the intended reader's desire to absorb several pages of rules and guidelines.

It's not uncommon for information security policy documents to run to dozens of pages, full of clauses and sub-clauses and often-irrelevant information for the average non-technical user.

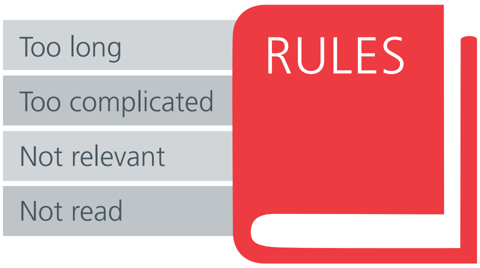
Clearly, it's important to get policy right. Over-complicating it however, will be counter-productive, as employees will not understand or implement the right security measures, or they will find workarounds. In the UK alone, 70% of companies where security policy was poorly understood had staff-related breaches versus 41% where the policy was well understood.

Information security professionals do believe in the importance of a good information security policy for users, but they are often forced to cut corners in developing policy. In a recent Kaspersky survey of IT professionals worldwide, 46% of respondents said they had insufficient time and resources to develop and implement IT security policies. It's not uncommon for policies to be cut and pasted from online examples with some tailoring of basic principles.

To effectively protect any business's most valuable information, IT professionals can't afford to compromise on their information security policy.

So what should you do?

Figure 4: The typical information security policy



KISS – Keep it Simple Security

Your employees are focused more on doing their jobs than they are on information security. This won't change and to protect your organisation's intelligence, it's prudent to accept cultural norms and aim instead for pragmatic guidance that is easy to consume and simple to follow.

Even the most security conscious organisations are adopting this approach. The UK Government is a case in point. It recently streamlined its security classification system, cutting seven tiers down to three in an effort to simplify its security policy and increase productivity.

Keep It Simple Security (KISS) is our approach to information security and it starts with the security policy for users.

Brainloop KISS categories:

1. Am I sure it's sensitive?

2. Am I sure it's not sensitive?

3. Could it be sensitive?

These three simple categories for sensitivity of information are easily understood and make it easy for users to choose: Yes, No or 'I don't know'.

Every organisation differs in size and complexity; you may need a few additional categories but aim to keep the number to a minimum.

Defining policy for what to do next with sensitive information also needs to be simple. A complex policy operation will still be disregarded, even if the classification categories are simple.

In the vast majority of businesses, users in possession of company sensitive information will be communicating with and sharing valuable information amongst people both inside and outside of the organisation – we believe the best security policy lets them continue to do so.

Allow users to continue to use the everyday processes and tools they are familiar with and build the right security environment and controls around it to protect valuable information.

> *<< About 80% of known attacks would be defeated by embedding basic information security practices for your people, processes and technology.>>*
>
> *Sir Ian Lobban, Director, GCHQ*

It’s time for change

Despite the unpredictability of when the next cyber-attack or security incident might occur, there are risk factors that IT chiefs can control to protect their organisation to the best of their ability.

In our experience, most businesses need to adapt their approach to protecting valuable information. The risk of a security breach is far higher from internal parties than external threats and this threat needs to be considered more carefully. Clearly, threat detection is an important component of reducing risk, but it can never be an absolute. Nullifying known internal threats can be controlled and risk eliminated completely with the right approach and tools. This shift in mindset might seem drastic, but it is certainly necessary.

Enabling employees to carry out their daily activities securely but without impairment should permeate every level of the organisation from top to bottom. Training on the dangers of carrying and sharing valuable or sensitive information will increase awareness of security measures, but minimising any responsibility for users to change their behaviour will be the critical factor in successful policy implementation.

Failing to address the risk posed by internal users leaves a business vulnerable to entirely preventable breaches and data loss. Remember, it’s quite possible that your most trusted colleague will unwittingly do more damage to your organisation that an anonymous hacker ever will.

> *<<The number 1 cause of security incidents in 2013 was current employees.>>*
>
> *The Global State of Information Security Survey 2015, PWC*

THREE GOLDEN RULES

1. *Be aware that information has value and it will leave your organization:*
   - Protecting intelligence is just as important as protecting infrastructure
2. *Make policy as simple to understand and operate as possible:*
   - Be aware that long, complex policies will be ignored
   - Take time to create a unique and simple information security policy
   - Appreciate that users are more concerned with getting the job done than security
   - Don’t ask users to change their work habits
3. *Understand that the internal threat is greater than the external one:*
   - Prioritise resources and time accordingly
   - Don’t dictate to your users, provide the right tools, educate and train them

Good security is simple security

Brainloop's expertise provides simple, secure collaboration tools that allow businesses to operate as normal with complete confidence around the safety and protection of their sensitive information and intelligence.

We make it simple for IT teams to implement security policies and integrate with existing systems such as SAP ERP, MS Office, IBM Notes without any change to the user experience.

We enable the encryption of all data in transit and at rest, and provide secure email to give businesses the assurance they need that critical information cannot leave the system, whether deliberately or accidentally.

Please get in touch to discuss how we can protect your business's valuable information sales@brainloop.com

About Brainloop

We provide a complete portfolio of highly intuitive SaaS solutions that enable our customers to securely manage and collaborate on confidential documents and information, whether inside or outside of their IT environments.

Brainloop's secure solutions look at the entire information protection issue in a holistic and integrated way to better protect the way businesses operate today. We go beyond common security measures to provide full 256-bit encryption, audit trail, two-factor authentication and provider and administrator shielding, all through an easy to use interface.

www.brainloop.com info@brainloop.com