

Lost in Translation?

Exploring the roots of miscommunication: strategies to ensure Information Security is on your Board's agenda.

Embedding Information Security into business-as-usual



“The security of corporate information will stand or fall by the ability of the organisation’s various functions to communicate clearly and effectively with one another. It takes all teams to sustain a meaningful dialogue, so a change in mindset is needed from all sides.

Business leaders ignore information security risk at their peril. Historically, business leaders and boards have tended to regard information security as a technology issue – as reflected by the traditional reporting channels – but this is a complete misconception and needs to change.”

Richard Sykes
PwC Governance Risk and Compliance Leader

Contents

2. A communication gap

- A key board-level risk issue
- The roots of miscommunication

5. Overcoming the language barrier

- Towards better communication
- Information owners accept responsibility

7. Embedding information security into business-as-usual

- Secure behaviour at all levels
- A processes-based approach
- Maintaining the momentum: strategy and operations

9 Five key steps for the business leader and security leader

11 A call to action

12 About PwC Onesecurity

13 Key contacts

Information Security: how to close the business communication gap

Real-world case studies

A courier carrying a large financial services provider's backup tapes was robbed. This led to several man-weeks of investigation to check that the data had not been misused.

A charity infringed data protection laws when it disposed of an old computer without wiping the hard drive. The staff member concerned was complacent, saying he had deleted the files and trusted the person to whom he had sold the computer.

A Midlands-based technology company lost a USB stick containing a customer's test data. Unfortunately, this resulted in extensive adverse media coverage over a prolonged period...and more than £100,000 in cash costs.

Source: Information Security Breaches Survey (ISBS) 2010, Infosecurity Europe/PwC

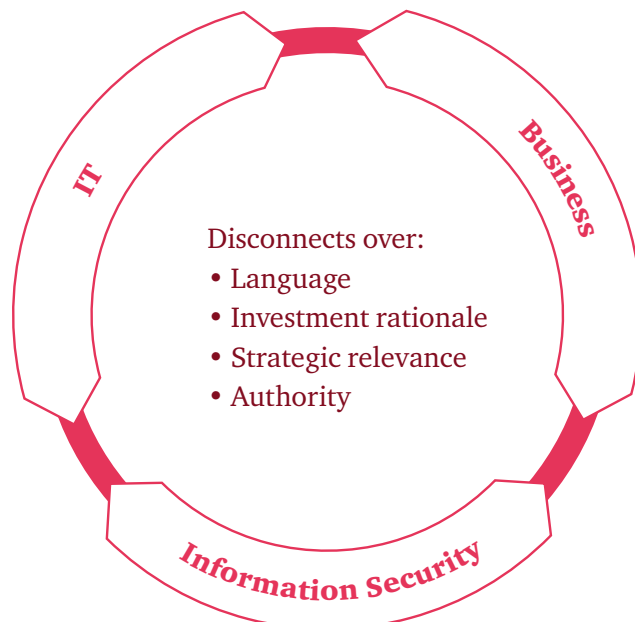
Recent research and an ongoing series of high-profile data losses have underlined the intensifying security threats to business-critical corporate information – with the result that business leaders are increasingly focusing on this major area of risk for their organisations. Yet in many businesses, a potentially catastrophic breakdown in communication between the Information Security and the business is undermining the ability to tackle this risk effectively.

In terms of the growing threat, recent statistics tell their own story. As the 2010 UK Information Security Breaches Survey (ISBS)¹ confirms, after declining for the past few years, a new wave of security threats is now hitting UK organisations, costing them billions of pounds.

Ninety percent of large organisations (more than 250 employees) have suffered a malicious security breach in the past year, and 46% have seen staff members lose or leak confidential data. In just twelve months, a typical large organisation has suffered 45 breaches costing up to £690,000 each. Furthermore, figures from the UK Information Commissioner's Office show that enterprises are running second only to the UK's National Health Service in terms of reported breaches, and are the main source of breaches from technical and procedural failures.

A key board-level risk issue

Historically, business leaders and boards have tended to regard information security as a technology issue – but this is a complete misconception and needs to change. The scale of the financial and reputational risks to a business mean that information security is now a key board-level risk issue, whose importance is also increasingly recognised by investors and regulators. In February 2010, the semiconductor manufacturer Intel became the first company to disclose a “sophisticated incident” of computer hacking in its 10-K filing to the US Securities and Exchange Commission.



1. 2010 Information Security Breaches Survey (ISBS), commissioned by Infosecurity Europe and written by PricewaterhouseCoopers LLP

The message is clear: business leaders today ignore or underestimate information security risk at their peril. Yet PwC's research and experience show that many organisations' ability to secure their mission-critical corporate information is being undermined by a communications gap between the three key participants in any information security strategy: the business units, IT, and Information Security department. Instead of working together towards common goals, these three stakeholders often fail to understand – or even respect – each other's roles and value to the organisation.

To gain insights into the how organisations can close the communications gap and make a fresh start in information security, PwC has collaborated with (ISC)² – the International Information Systems Security Certification Consortium – to research information security's role, including conducting a round-table with industry leaders. We have distilled the findings to create this point of view paper, which includes useful insight from the participants at the round-table and a call to action.

The roots of miscommunication

So, why does this breakdown in communication arise – and what are its impacts? Let's analyse the psychology of each of the three key stakeholders in this relationship: the business, IT, and Information Security.

The business

The business knows it provides the revenues that ultimately drive profits for the organisation. As a result, it has a cast-iron certainty that it is much more important than both IT and Information Security. It accepts – grudgingly – that IT provides vital support to its processes, but it frequently feels frustrated at time and costs incurred in even small changes to business systems. Worryingly, the business's disconnect from Information Security is even greater, since it does not see a real business need for the function's existence, and cannot understand much of what it says.

In the business's view, the role of Information Security is to make its life as difficult as possible, with obscure policies and complex restrictions that hinder the conduct of normal business.

“There's a difference between IT security and information security, particularly in terms of organisational responsibilities. People in IT are probably best placed to understand IT risk. But you need business people to understand the risks around information, and to take some responsibility for managing them.”

Jeff Brooker Head of Security & Business Continuity HMRC

“Language is the biggest barrier. In Security we don't speak business language – so what seems clear to us can sound like double Dutch to the people we are speaking to in the business... Adding 'risk' to my job title has been very useful. The business understands risk.”

Stephanie Daman, Information Security Risk, HSBC

“As head of Information Security, you need to know about encryption, firewalls and so on. But if you go to the Board and talk that language then you’ll lose them immediately. Security is about people, and if people are not interested or engaged by what you’re saying then you won’t influence them.”

James Gay, Chief Information Security Officer, Travelex

The IT department

The IT department also believes it is the most important function in the organisation, since the business would be unable to operate without it. However, IT also feels that the business does not really appreciate the good work it does – especially since it is always being pressurised to deliver new systems and changes in impossibly short timescales. In IT’s view, the Information Security department makes its life even more difficult, by insisting on extra controls in business systems, and delaying the implementation of completed projects by insisting on ‘time-wasting’ activities such as penetration tests and code inspections.

The Information Security department

For its part, Information Security believes that it fulfils the most important function, because it protects the enterprise from cyber attacks and related risks ranging from regulatory penalties to reputational loss. It realises that it is unappreciated and disliked by both the business and IT, and cannot understand why they fail to understand the importance of its role. It also feels – quite rightly – that the three functions should be partners fighting on the same side against a common threat. Yet when it tries to explain the nature and scale of the threats facing the business and IT, it comes up against misunderstanding and incomprehension. In some industries, such as financial services, regulatory and compliance pressures have helped Information Security ‘sell’ security to the business and get onto the business agenda. But in most sectors this remains an uphill battle.

However recent research indicates that change is now under way, with organisations reviewing the reporting lines between Information Security and the Board. Traditionally, Chief Information Security Officers (CISOs) have reported in to the CIO – an approach that has tended to limit both their authority and effectiveness. However, according to the 2011 PwC Global State of Information Security Survey, CISOs’ reporting lines are now shifting towards other Board members, including the CEO and CFO. This appears to signal a growing executive recognition that security’s strategic value should be more closely aligned with the business than with IT.

Who the CISO reports to	2007	2008	2009	2010	Three-year change*
Chief Information Officer	38%	34%	32%	23%	- 39%
Board of Directors	21%	24%	28%	32%	+ 52%
Chief Executive Officer	32%	34%	35%	36%	+ 13%
Chief Financial Officer	11%	11%	13%	15%	+ 36%
Chief Operating Officer	9%	10%	12%	15%	+ 67%
Chief Privacy Officer	8%	8%	14%	17%	+ 113%

Source: 2011 PwC Global State of Information Security Survey

Overcoming the language barrier

These findings suggest that many organisations have identified the communications gap between business and IT, and are trying to close it. If you are leading a business where this gap still exists, there is no time to lose. You know that protecting corporate information is vital to the wellbeing of the business. You also know that it takes multiple participants to create and sustain a meaningful dialogue, so a change in mindset is needed on each side.

In acting to close the gap, it is important to understand that the roots of this communications breakdown generally lie in the different language used and understood by the three parties. The importance of good security practice has been recognised by many companies, resulting in security awareness programmes seeking to encourage better communication, heighten awareness and establish best practice behaviours. Yet few organisations would claim that these have been truly successful and more work needs to be done.

Towards better communication

To improve the outcomes of these initiatives, it is important to establish in advance what will be communicated, who the recipients will be, and what mechanisms or channels are available to deliver the messages. This information enables the appropriate resources to be identified and marshalled to execute the information security communications strategy.

The programme should aim to articulate the critical importance of the organisation's critical corporate information – ranging from customer databases to vital intellectual property – and to highlight the impact on the business should these assets be compromised. This means answering questions such as:

- What information is most critical, and where and how is it held?
- Why does it matter to everyone in the business that this information is kept secure?
- Can the business place a value on this information in both financial and reputation terms – and, if so, what is it worth?
- What security risks does this information face, and what safeguards are in place to mitigate them?
- What would be the financial, reputational and regulatory impacts on the business if the information were compromised?
- Is the culture “need to know?” or “need to share?”

Focusing on the questions such as these will focus attention on the true value of – and risks to – your organisation's critical corporate information, and automatically help to build a greater understanding and awareness of the need for security. Once this information has been given an explicit value, it becomes more tangible to the business, in turn making the importance of information security more obvious.

“In Information Security, we have to show we understand the business's roles and objectives, and that we are a supporter, not a detractor. We can do this by using tangible examples of how we can help the business with the P&L.”

– Mark Wolsey, Director Global Security, Cadbury

“We've found that the way to engage the business is to talk about risk – not about firewalls, encryption or penetration testing. Just point out a few scenarios, such as what would happen to the reputation of the company if we lost some of our most critical data. And send them home thinking about it.”

Bob Harris, Chief Technology Officer, C4

Information owners accept responsibility

This understanding of the business value of data also helps to drive a further shift in the relationship between Information Security and the business, by placing the responsibility for securing the assets with the data owner, not the security practitioner. As a result, Information Security can be transformed in the eyes of the business and IT from an irritant into a vital resource for achieving business aims, managing risk and protecting value.

The biggest challenge for Information Security in trying to achieve and sustain such a role is that it demands a new mindset and vocabulary. The security practitioner must be able to converse with the business, understand the issues and risks from the business's point of view, and protect its digital assets proactively – while simultaneously supporting the use of new technologies to open up new business opportunities.

Embedding information security into business-as-usual

Companies that successfully reshape and clarify the relationship between the business, IT and Information Security in this way can embed information security into their business-as-usual – thereby transforming the effectiveness and robustness of their defenses.

This embedding marks a breakthrough for the entire business. By removing the communication barriers that have previously hampered Information Security's relationship with the business, the corporate leadership gains the ability to establish a truly secure organisation – one that is resilient, adaptable and responsive to changing threats.

The litmus test: secure behaviour at all levels

Such an organisation has information security thinking, practice and behaviour deeply embedded as an integral part of its day-to-day operations and decision-making. The litmus test is when information security can be seen working at all levels – effectively woven into everything done by everybody inside and connected with the business, with minimal day-to-day intervention needed from security practitioners.

When an organisation achieves this degree of embedding, employees and trading partners unconsciously think and operate in a secure manner, and the right technical measures are in place to unobtrusively support secure operations. So being secure becomes a 'given' that underpins all business processes and relationships.

A further important step towards embedding information security behaviour is to tie security awareness more widely into other corporate programmes. Various activities that may previously have been regarded as unrelated to information security – such as training around anti-money laundering measures, ethical codes of conduct and regulatory compliance – have clear overlaps and linkages with the information security agenda and mindset. More and more organisations are aligning and linking these formerly distinct programmes to optimise the overall impact on behaviour.

“To date, a lot of the interest in information security at Board level seems to have been driven from the regulatory side... The fact that Boards simply go out and buy iPads (or Blackberries a few years ago), and then want to plug these new devices into corporate systems, highlights there's still a lack of understanding of the dangers around information security.”

Steve Marsh, Office of Cyber Security and Information Assurance, Cabinet Office

“We have to translate the language of security into the language of risk. And it’s hard to do that unless you link it to £ or \$, and say: ‘If this information is compromised, it affects your top or bottom line in this way’.”

Dr Gerhard Knecht, Head of Global Security Services and Compliance, Unisys

“For us, one of the biggest drivers is our clients’ security requirements. We align what we do with our clients, and that drives our business. If you are working on technology enabled business projects with a bank, then your information security must be at least as good as the bank’s. And the bar is constantly rising.”

Lawrence Guedes, Group Legal Director, Logica

A processes-based approach

More generally, reaching the stage where information security thinking is truly embedded requires two elements: a process-based approach to information security, and close cooperation with business process owners.

Both requirements can be supported through proactive groundwork carried out by Information Security. By investing up-front in an ‘under-the-radar’ analysis of business processes, the Information Security function can develop a compelling model and business case for further actions to present to the business process owners, including detailed process analysis, security requirements definition and ultimately new controls.

This requires a close understanding of what these processes are, both in terms of the business goals they serve, and also their inner workings – the individual steps, information flows and technologies within each process. Such detailed insight into the key processes enables well-informed decision-making on selecting, implementing and operating the right controls in the appropriate places in a cost-effective and risk-aware manner.

Maintaining the momentum: strategy and operations

To sustain and improve the organisation’s information security further over time, the business leadership needs to ensure that the Information Security function maintains a focus on both the strategic and operational agendas.

In terms of strategy, Information Security needs to be able to anticipate and prepare for the forthcoming risks that will arise from the changing landscape of risk. This means continually scanning the information horizon to identify not just new threats, but also new technologies that may add value to the business, and identifying how both will be accommodated into the organisation’s security environment. No information security leader should be caught by surprise when the Board go out and buy iPads.

In terms of operations, Information Security must continue to work closely, collaboratively and responsively with the business process owners and with IT to support both functions in achieving their business objectives. This role as a collaborative enabler – rather than a proscriptive barrier – will sustain and build the business’s confidence and buy-in for what Information Security is seeking to achieve. In PwC’s view, this approach provides a more workable basis for embedding information security than the more prescriptive ‘secure-the-perimeter’ model that was traditionally employed in the past – but which is now being rendered increasingly obsolete by the rising interconnectivity across today’s value chains.

Making a fresh start: five key steps for the business leader and security leader

If – as a business leader – you find that our description of the three-way communications gap resonates within your own organisation, then it is time for a fresh approach to Information Security. The current impasse is hampering the business's ability to engage constructively and intelligibly with Information Security to ensure the business's vital information is protected effectively. It follows that it exposing the entire organisation to unnecessary risks. Clearly, it is the duty of the business's leadership to sort this situation out.

To help them do this, they should ensure that the organisation's information security risks are being assessed and managed within the context of its wider Enterprise Risk Management (ERM) framework. Historically, there was a tendency for information security professionals to focus on their own specific risks, without reference to the wider ERM agenda and actions. Instead, the Information Security function should explicitly tie and map information security risks into ERM. Similarly, the ERM function should make sure it is up-to-date with the risks in information security. Fortunately, our experience shows that this is increasingly the case.

With this need for linkage to ERM in mind, here are five steps that business leaders can take to help close the information gap and secure critical corporate information more effectively – and five corresponding actions they should look for from the organisation's information security leader.

“The demand pull for security is there now from the executives and the business. So it's about creating an environment where they can really understand the issues.”

Robert Coles, CISO & Head of Digital Risk & Security, National Grid

What you should do as the business leader

What you should expect from your information security leader

1. Highlight the risks – perhaps by citing examples from recent high-profile breaches – to show the importance of information security within the wider ERM landscape, and to engage the whole Board in the need for world-class information security standards. Hold a Board briefing with the information security leader on current and emerging business threats and solutions.
2. Discuss future strategic technology choices and trends at Board and senior executive level, pinpointing potential forthcoming changes in areas such as device and application usage. Then involve the security leader in assessing the impact and implications if these shifts happen.

- Ask the information security leader to avoid using complex technical language and to describe business risks and the relevant controls in straightforward business terms. Ensure he or she uses this business – and risk-focused approach to reach out to key internal clients, understand their perspective on security and explain solutions.
- Task the information security leader with continually scanning the horizon of emerging devices and cyber threats from the perspective of the business's strategic objectives and opportunities. For example, if electronic tablets or viral marketing via social networks could be on the agenda, then ensure the information security leader assesses the security implication now, rather than waiting until these innovations start appearing in the business.

-
- | | | |
|-----------|--|---|
| 3. | Rate your organisation's various business units from an information security perspective, on a scale from low to high risk. For those that are high risk, consider expanding the senior executive's bonus calculation to include success in implementing top-level security standards. | Ensure that your information security leader analyses your organisation's underlying business processes from an information security perspective, and then develops proposals for more relevant, cost-effective and value-supporting controls, supported by clear business cases. |
|-----------|--|---|
-
- | | | |
|-----------|---|---|
| 4. | Initiate an ongoing series of joint workshops or forums with people from Information Security, business and IT, to brainstorm the threats and opportunities and debate solutions. | Support the information security leader in forging strong links with 'natural allies' in the business such as Legal, Compliance, Risk and Internal Audit. This might include aligning Information Security closely with areas such as operational business risk, to the extent of picking up their business-focused language and reporting templates. |
|-----------|---|---|
-
- | | | |
|-----------|---|--|
| 5. | Over the longer term, engage the security leader more deeply in the strategic agenda and future plans, enabling Information Security to plan proactively into the future rather than reacting to emerging events. | Continue to engage and ensure that Information Security's key business role and relevance is understood and appreciated throughout the organisation, so it is regarded as a source of business-enabling solutions rather than a barrier to doing business. |
|-----------|---|--|
-

To truly protect the critical information at the heart of today's organisations, all parties involved – the board, the business, IT and Information Security itself – need to speak the same language: the language of business operations, opportunities and risks. As the threats to information continue to intensify, the security of corporate information will stand or fall by the ability of the organisation's various functions to communicate clearly and effectively with one another. Business leaders must set the right context in which this communication can take place.

To help you to assess and evaluate if you have the appropriate level of Information Security for your business, consider asking IT, the business and Information Security the following questions and then compare the answers. The results will most likely be both surprising and useful.

Call to action

- 1.** Do you have an up-to-date Information Security strategy that is aligned and mapped to the specific needs of the business?
- 2.** What are the primary drivers that impact your information security spend?
- 3.** Do your information security managers have clearly defined roles and responsibilities, with the appropriate reporting lines within the business?
- 4.** How do you measure performance and ensure it is in line with the business needs?
- 5.** Do you have a cross-organisational team or forum that meet to coordinate and communicate information security issues on a regular basis, including senior management from finance, legal, risk, human resources, as well as security, technology and even public relations?
- 6.** Does the audit committee review the effectiveness of information security on an annual basis?
- 7.** Is the process for identifying and managing risks at an enterprise level connected to information security effectively?
Are weaknesses addressed quickly?
- 8.** Are there top level policies for creating a culture of security?
Do you have an embedded corporate responsibility for protecting your business?
- 9.** Do you know what data you hold and what its value is to you?

About PwC OneSecurity

The PwC OneSecurity team has over 30 years' experience in all aspects of security, from espionage to governance risks. Our globally based team understands and speaks business language, we know when and how best to involve experts in legal, IT, business continuity, disaster recovery, crisis management, fraud, forensic and human resources expertise. This wide range of know-how means we can help your organisation to devise a dynamic and forward-thinking security strategy that identifies the security risks you face, and offers practical and effective ways of ensuring they are addressed. PwC were recognised as a leader in Information Security and Risk, by Forrester in 2010.



Contacts

To have a deeper conversation on specific issues mentioned in this paper, please contact:

Grant Waterfall Partner, Leader IT Assurance
grant.waterfall@uk.pwc.com
+44 (0) 7711 445 396

William Beer Director, OneSecurity, Risk Assurance
william.m.beer@uk.pwc.com
+44 (0) 7841 563 890

A special thank you to John Colley and Graham Mann from (ISC)² EMEA, who made a significant contribution to the content of this paper.

