
ISSA-UK

Information Security - The Next Decade

December 2010





PREFACE

This paper is a timely reminder that awareness is a continuing task, both for individuals and for business. Much work has taken place (for instance, in Yorkshire and the Humber) on informing and increasing information awareness for small businesses.

The continuing lesson is that the tide comes in and the tide goes out. There is a substantial effort to increase awareness, followed by a return to relative complacency.

As in so many things, the role of government is ambiguous. As with the banking system, there is a clarion call that government should not be overbearing, should not regulate or interfere. In the next breath, it is also 'someone' who should have done something to ensure that security and protection on the one hand and information and advice on the other, was properly delivered.

This balance and proportionality is part of the debate of increasing understanding and ensuring that individuals and business play their part in being the solution and not the problem. Therefore, balancing responsibility with duty, the importance of light-touch but effective frameworks on the one hand and individual ownership of identity and transferability on the other, really does matter.

The State may on occasions be part of the problem, but it also has to remain part of the solution.

Rt Hon David Blunkett MP

ISSA-UK Advisory Board Chairman

THE NEXT DECADE OF INFORMATION SECURITY

The ISSA-UK Advisory Board, together with some of the UK's top information security thought leaders, met in October 2010 to discuss "The next decade of Information Security". The meeting, held at the House of Commons and chaired by the Rt. Hon. David Blunkett MP, resulted in a fascinating and engaging exchange of views. The debate was wide-ranging and controversial, as might be expected from a diverse group of stakeholders, policy makers and specialists. This report sets out some of the key issues discussed.

A list of attendees and contributors is attached.

A growing threat landscape

Regardless of who we judge to be the enemy, whether it is organized crime, hostile intelligence agencies, or simply human failures in operating information systems, it is clear that the security community faces a growing challenge in countering emerging threats. Thefts of government and industrial secrets have reached unprecedented levels. Identity information is the new currency. Trade secrets are the growing target of many intelligence services. And losses of mobile devices containing large amounts of sensitive data have become commonplace.

"In the last ten years, we've gone from a threat environment of high impact but low probability risks, to something akin to the Wild West"

The technical capability of criminals has become alarmingly sophisticated, not only in the way they mount attacks, but also in the way they share, exploit and safeguard their techniques and data. When it comes to information sharing, organized crime is agile and innovative. As one expert put it "Business can't link data, but criminals can". Criminals are also highly sophisticated at hiding data to frustrate investigators. These trends are likely to continue.

This new intensity and professionalism in the threat landscape has taken many organizations by surprise. Few risk management functions would have anticipated a rise of this magnitude in information security threats. As one expert put it, "In the last ten years, we've gone from a threat environment of high impact but low probability risks, to something akin to the Wild West".

Supply chain exposures are also beginning to present a new level of concern. They are the 'elephant in the room' that we choose to ignore. As one expert put it, "Where is the next big threat? Is it Chinese hardware, Indian software or insider threats?" Certainly no enterprise can withstand a strategic attack mounted through a trusted supplier or insider. The Stuxnet worm has demonstrated that even the most protected of environments can be penetrated by a determined, sophisticated attacker.

In the future, criminals and terrorists are also likely to exploit exposures that can result in damaging impacts to business, such as attacks on the integrity of databases and information systems. Modifications to software and data can create lasting damage to business services and corporate reputations, though the prospect of such incidents has yet to appear on the radar of most enterprises.

To respond to this emerging threat landscape, the security community requires no less than a quantum leap in its capability to tackle attacks that are becoming progressively more strategic, professional and sophisticated.

The coming 'information tsunami'

In the next decade, not only will we face stronger and smarter threats, we can also expect to be awash with growing waves of information. Data is becoming 'superabundant': growing at a massive rate (60% per year according to the Economist). Some of this information is also sensitive, valuable, critical to business, and increasingly communicated, stored and processed outside of corporate perimeters.

"With Moore's laws for processing, storage and the amount of information being produced, we haven't started to do information security yet. Just about every design principle and people-based security process isn't going to scale for much longer and certainly not for the next 10 years."

Growing numbers of people will have greater access to larger volumes of data. Cloud computing services will enable much larger amounts of data to be stored and processed efficiently. Information will become considerably harder to manage. And, at the same time, its value and attractiveness will increase with the growing use of data mining techniques and the increasing exploitation of personal data for fraud, espionage and marketing. The growing difficulty of removing data, once created, will become an increasing concern to citizens.

As one research expert put it "with Moore's laws for processing, storage and the amount of information being produced, we haven't started to do information security yet. Just about every design principle and people-based security process isn't going to scale for much longer and certainly not for the next 10 years. Anybody who claims otherwise doesn't understand the information tsunami that is coming." Organizations will not be equipped to manage future demands. Security managers will need to run faster and faster to keep abreast of the growing volume and complexity of business security demands.

The challenge of SME security

Small and medium enterprises (SMEs) are increasingly being used as suppliers by larger corporate businesses and government ministries. Very few SMEs, however, have the awareness, motivation and capability to apply contemporary information security safeguards. Current security standards and products are aimed primarily at large organizations with greater security skills, experience and resources.

"SME suppliers are the soft underbelly of big business and critical national infrastructure"

This lack of security in SMEs presents a growing vulnerability in industry and government supply chains. SME suppliers represent "the soft underbelly of big business and critical national infrastructure". Greater efforts must be made to encourage and help them to address information security risks.

The ISSA-UK currently has a working group addressing this challenge. It has already identified the need for new standards, incentives and outreach initiatives, and action has commenced to help address these requirements. Many security vendors are also considering this market as a potential recipient of low cost, cloud based services. 2011 could be a turning point in efforts to bring SMEs up to speed with security.

Technology trends spell the end of security perimeters

Technology trends such as consumerisation, mobile computing and cloud computing are relentlessly dissolving existing physical, electronic and lifestyle perimeters, removing the primary, traditional lines of corporate security protection. Many of today's information systems, however, remain highly vulnerable when operating outside of a protected, private environment. Traditional fortresses don't work in the new societal construct.

"Traditional fortresses don't work in the new societal construct"

Organizations have yet to fully embrace security solutions that operate at the data and application levels, however, continuing to rely on infrastructure level security controls that might not be available, or as effective, in a public or shared network environment.

A particular concern is that much of the critical infrastructure that supervises or controls vital business, government and citizen services is now connected to public networks, though the platforms used to support these services were not designed to operate in a hostile, public network environment. This exposure is likely to be further intensified as corporate infrastructures migrate to cloud computing environments.

Unfortunately, the typical response to publicized security exposures is to apply quick operational fixes, rather than address the long term, underlying weaknesses in system development processes. This trend is likely to continue, as tight budgets combined with a short term business perspective will discourage investments in any initiatives that do not deliver an immediate return on investment.

Objectives - what should we be trying to achieve?

"Are we aiming to help catch the bad guys, minimize losses, stop bad things happening, make the world a safer place or simply react to events by offering a timely response?"

"Revolution or evolution" was the title of a recent future information security 'roadmap' commissioned by the Technology Strategy Board and jointly prepared with PWC. The research examined the impact of technology trends, such as feature rich mobile devices and faster broadband access. Amongst other things, the analysis envisaged an increase in crime and increasing pressure towards regulation in information security, with privacy and consent being key drivers. Proving identity and establishing trust were judged to be two of the greatest future challenges, as people spend an increasing proportion of their time online, with fewer face-to-face interactions.

A key question was who should take the lead in determining what needs to be done. But that depends on what we are trying to achieve. Are we aiming to help catch the bad guys, minimize losses, stop bad things happening, make the world a safer place or simply react to events by offering a timely response? Security means different things to different stakeholders. And the work has to be done with a progressively smaller budget, against a landscape of growing complexity. We will certainly need to 'work smarter' to stay on top.

Regarding process, it was felt that security has a tendency to impose solutions that are not really welcome. There is too much emphasis on controls, and insufficient on the people who use the technology. Users don't want to be restricted in their actions, but they need advice on what is safe. Ideally, we should aim to make the individual a discriminating buyer of appropriate services, rather than a passive recipient of difficult-to-understand security barriers.

Responding to the challenge – who takes the lead?

There was general agreement that addressing the growing problem space requires a cooperative rather than an imperial approach to governance. Traditionally, citizens have looked to government to take care of national security concerns. Cyber security is different, however, in that government needs to look to industry for solutions and action. There are precedents for this however. “The Wild West wasn’t tamed until the Pinkerton detective agency took action”.

“The biggest threat is us - doing nothing”

A further point is that “Government is not always a good governor”. Privacy continues to be a major concern of the public, even for young people, who want to be online, and want it to be safe. Some observers view government as presenting a significant threat to privacy, however, through excessive intrusion and eavesdropping. Government is therefore not best placed to regulate. As one expert put it, “We should not give government agencies a permit to hunt”.

The Internet is a new societal construct with as much impact as the printing press. It transcends nation states and geo-political power, and may even lead to a unity of national governments. We need to see and manage it in this context. Conventional discussion has looked at it from a mathematical or computer science approach. We should look at it from an anthropological, sociological view. Education was also a key issue, where it was felt we needed to break the current situation where knowledge of information security is held by a relatively small number of individuals.

Experts were divided on the issue of whether practitioners should on the one hand pool resources, coordinate effort and avoid duplication, or on the other encourage innovation through competition. There was a strong appetite for better leadership, organization and control. But there were also pleas for greater diversity and competition, to enable innovation. The debate indicated there are advantages and risks associated with both approaches. The learning point is that the implications of interventions need to be carefully considered. There are as many dangers in adopting a herd mentality, as in turning a blind eye to a proliferating state of anarchy. But the biggest threat, as one expert put it, “is us - doing nothing”.

David Lacey, Director of Research, ISSA-UK

November 2010

ATTENDEES AND CONTRIBUTORS

Rt Hon David Blunkett MP (Lab) (Advisory Board Chairman)

Dr. John Meakin (Joint Dep. Chair)

Dr. Steve Marsh

Paul Simmonds

Earl of Erroll

Philip Virgo

Andrew Yeomans

Rt Hon Alun Michael JP MP (Lab)

Martin Sadler

John Colley

Sarb Sembhi

Lord Toby Harris

Professor Sadie Creese

Andrew Martin

Neil Stinchcombe

David Lacey

Charlie McMurdie

Tom Scholtz

Geoff Harris (ISSA-UK President)

Roger Ellis (ISSA-UK Treasurer)

Raj Samani (ISSA-UK VP of Ext Communication)

Les Fraser (ISSA-UK VP Scottish Region)

Andrew Cunnington (ISSA-UK Management Team)

Dr. John Leach

Jon Colombo

Colin Williams

Duncan Curry

Professor Ross Anderson

William Beer

Dr. Alex Baxendale

Mark Chaplin

Bob Ayres

Martin Smith MBE

Professor Peter Cochrane OBE