Success and profitability:

Security and the value of IT/business solutions

Michael O'Neil
Principal Analyst
InsightaaS.com
August 2014

An InsightaaS.com
whitepaper sponsored by: DELL

Executive summary

The premise of this paper – that effective IT security solutions contribute to organizational success and profitability – rests on two assumptions:

- IT/business solutions are important to business success and profitability; and.
- Security is important to the value of IT/business solutions

Most business executives would agree broadly with the first point, or would at least concede that the *absence* of effective IT/business solutions impedes business success. The second point is less intuitive; in many environments, IT security is viewed as a necessary-if-unwelcome cost, rather than as an enabler of business solutions, a viewpoint that is reinforced by the clear need for IT security in the face of increasing threats to information security and business continuity. This need not and should not be the end-point of the IT security discussion, though. Effective security practices go beyond merely 'raising the shields' around users, data and networks – they enable innovation throughout the IT/business infrastructure. Environments where security acts as an anchor will not be agile, will have difficulty innovating, and are likely to fall behind more nimble competitors. Organizations that build effective, responsive security frameworks will be positioned to capitalize on new technologies and on the new efficiencies that they enable.

Research from McKinsey & Company shows that "cybersecurity…is a CEO-level issue." CEOs may become engaged with security because they are fearful of the customer, shareholder and regulatory consequences of a data breach – but ultimately, CEOs are paid to drive growth and profitability. Capitalizing on C-suite interest and the increasingly-sophisticated products and services offered by suppliers, IT security-responsible managers are positioned to bolster organizational agility and performance – and their own career arcs – by recognizing and meeting the requirement for security to be a powerful factor in overall business success.

Contents

Executive summary 1

Contents 2

The growing importance of business IT 3

IT is pervasive – and becoming more so.................... 4

On balance: IT matters to business success, and security matters to IT success............................ 5

Coming to grips with the downside of connected systems.. 7

The impact of a breach.. 8

Management approaches suffer from an important disconnect 8

Netting out the downside of security threats............ 9

IT security options and upside..................................... 11

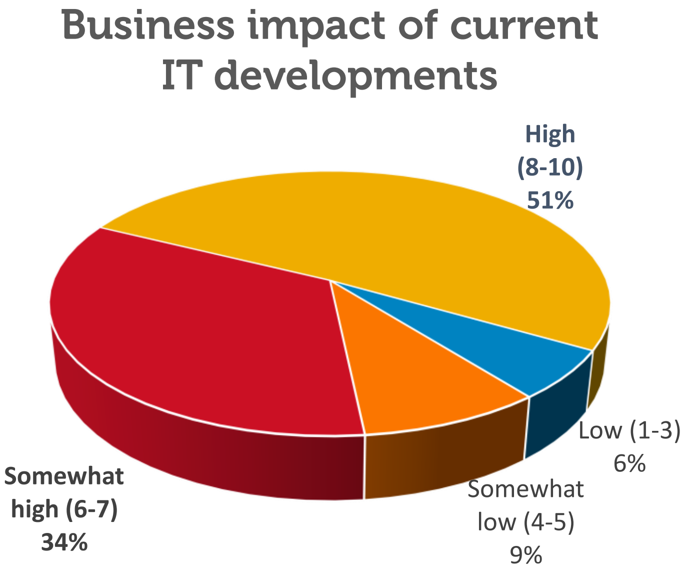
Netting out the “good news/bad news” security equation.. 12

The growing importance of business IT

It is evident from even a casual tour of a modern office that IT has become integral to business activities. Email and communications systems that meld conventional, web-based and mobile phones, and social collaboration tools on the web and within our offices provides the basis for connections between companies and customers, across processes and with suppliers, and between staff members. Productivity applications like spreadsheets, graphic presentation packages and word processors enable us to complete tasks and document progress, while enterprise applications capture and report on financial data and organize processes.

Given the nearly-ubiquitous nature of IT, it's fair to wonder: are we 'there' yet? Have we deployed all of the technology that we need? Results from a recent survey of 635 Canadian IT managers (ITDMs) and business decision makers (BDMs) conducted by California-based research firm Techaisle indicate that there is still a voracious appetite for new IT-based business solutions. Asked to evaluate the business importance of current IT developments, more than 50% of survey respondents reported that new IT systems would have a high impact (8-10 on a scale of 1-10), and an additional 34% believed that new IT developments would be somewhat important (a rating of 6-7) to their organizations. Only 6% believe that new IT products and services will have little impact on their businesses. Clearly, Canadian BDMs and ITDMs agree that new technology will play an important role in making their businesses more profitable, and their employees more productive.

Figure 1. The business impact of current IT developments

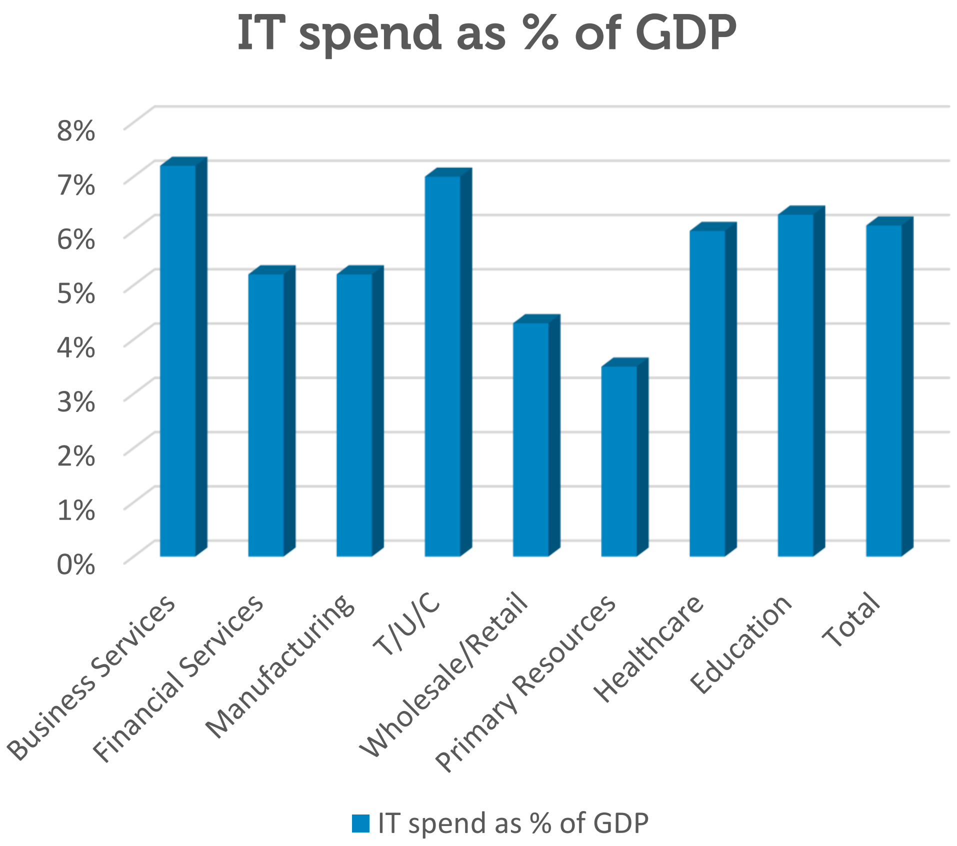


Source: Techaisle survey of 635 Canadian ITDMs and BDMs, December 2013

IT is pervasive – and becoming more so

The evidence of IT's ubiquitous presence is not limited to the anecdotal evidence found in a review of office activity – it is also seen in the financial allocations of Canadian public and private-sector organizations. Market data from InsightaaS shows that in 2012, IT spending accounted for just over 6% of total Canadian GDP – and as Figure 2 illustrates, IT spending is significant across all industry sectors. It isn't an exaggeration to state that in today's business world, IT infrastructure *is* business critical infrastructure. Businesses are heavily invested in IT, with IT-dependent processes throughout their operations. This ubiquitous dependence on technology means that systems failure will reverberate throughout all of a company's daily operations. There's no way to disaster-proof against IT failure with insurance; appropriate investment in IT security processes, technologies and management strategies is the only way to capitalize on the productivity benefits of IT without creating exposure to organizational paralysis in the event of a malware invasion, a hacker attack or an employee's negligence or malfeasance.

Figure 2. IT spending as a proportion of GDP

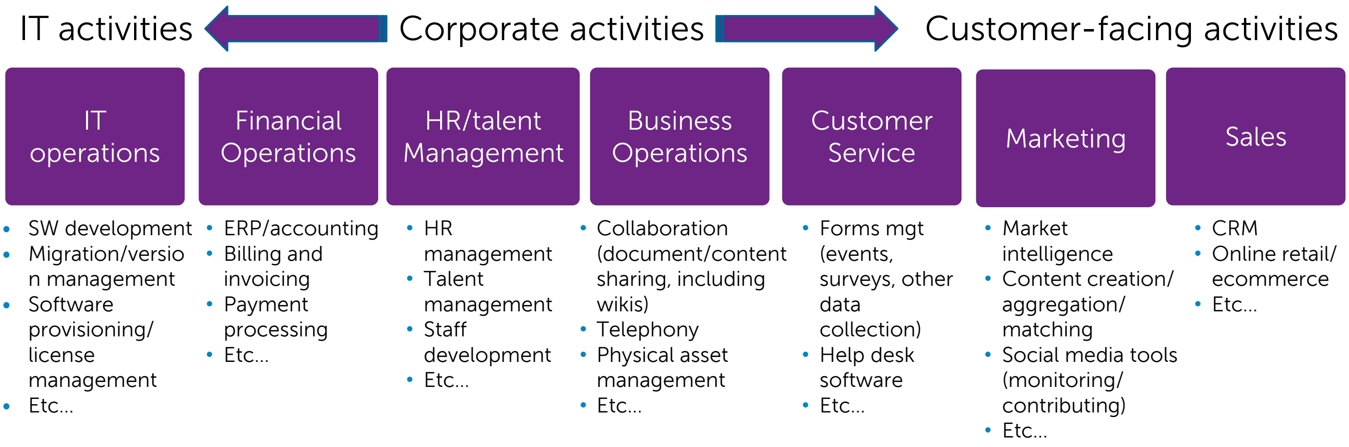


Source: InsightaaS. GDP figures from Statistics Canada, in 2007 chained dollars. Public administration included in total but excluded as a discrete category

The statement that concludes the previous paragraph – roughly, "appropriate investment in IT security…is the only way to capitalize on the productivity benefits of IT without creating exposure to organizational paralysis" – reflects the most common perspective on security: that it is a 'necessary evil,' a type of tax on IT enablement. But there is another way to look at the issue. Organizations that invest in building responsive and capable IT security infrastructure and practices are able to move more quickly and surely than their competitors to adopt new technologies in new areas.

A sound argument can be made that because of cloud computing, this capacity for rapid technology adoption is more important today than ever before. With cloud, the cost of developing and marketing new applications has dropped by at least 1-2 orders of magnitude – and with that reduction in cost has come a proliferation of new applications. These new offerings enable automation in areas that previously could not be addressed, because the cost was too high and/or because the market too diffuse or ill-defined. Today, though, it is possible to acquire solutions that address any combination of IT, back-office and customer-facing tasks. Firms that can adopt these applications and orchestrate across them, tying them into a coherent IT/business architecture, can gain new capabilities, improve process efficiencies and/or reduce costs much faster than their competitors. However, each new application creates a need to secure users, data, and the environment that the solution integrates into. This conjunction of opportunity and exposure illustrates the connection between business success and effective IT security: firms that build robust frameworks can capitalize on the opportunities highlighted in Figure 3, while those that treat security as an onerous requirement that is invoked each time a new system is contemplated will be slow to adopt – and profit from – new IT-enabled business process efficiencies.

Figure 3. Cloud-based options for improving business processes



IT activities ← Corporate activities → Customer-facing activities

IT operations
- SW development
- Migration/version management
- Software provisioning/ license management
- Etc…

Financial Operations
- ERP/accounting
- Billing and invoicing
- Payment processing
- Etc…

HR/talent Management
- HR management
- Talent management
- Staff development
- Etc…

Business Operations
- Collaboration (document/content sharing, including wikis)
- Telephony
- Physical asset management
- Etc…

Customer Service
- Forms mgt (events, surveys, other data collection)
- Help desk software
- Etc…

Marketing
- Market intelligence
- Content creation/ aggregation/ matching
- Social media tools (monitoring/ contributing)
- Etc…

Sales
- CRM
- Online retail/ ecommerce
- Etc…

Source: InsightaaS.

On balance: IT matters to business success, and security matters to IT success

The evidence presented in this section points clearly to the fact that IT is important to business success, and that it will play an increasingly important role in business success in the future. The link between security and business success is less transparent, but it is evident nonetheless. If security is viewed as an 'anchor,' management will be constrained in capitalizing on IT-enabled business system potential by a governance framework that is too slow and unwieldy to keep pace with emerging opportunities. The graphic that provides a summary for this section (Figure 4) shows that while there is upside and downside from a business/security perspective, on balance, security is an enabler of business success and profitability.

Figure 4. On balance: IT security and the growing importance of IT solutions

Good News:

- IT maters to business success
- Businesses are investing heavily
- IT will continue to increase in importance
- IT is business-critical infrastructure

Bad News:

- Interruptions in IT service will be felt – clearly and immediately
- There's no real way to disaster-proof IT
- The impact of IT failure has expanded tremendously

<u>THE VERDICT:</u>

- *IT security has the potential to become a high-value, strategic activity, rather than an 'anchor' or cost of doing business*

Coming to grips with the downside of connected systems

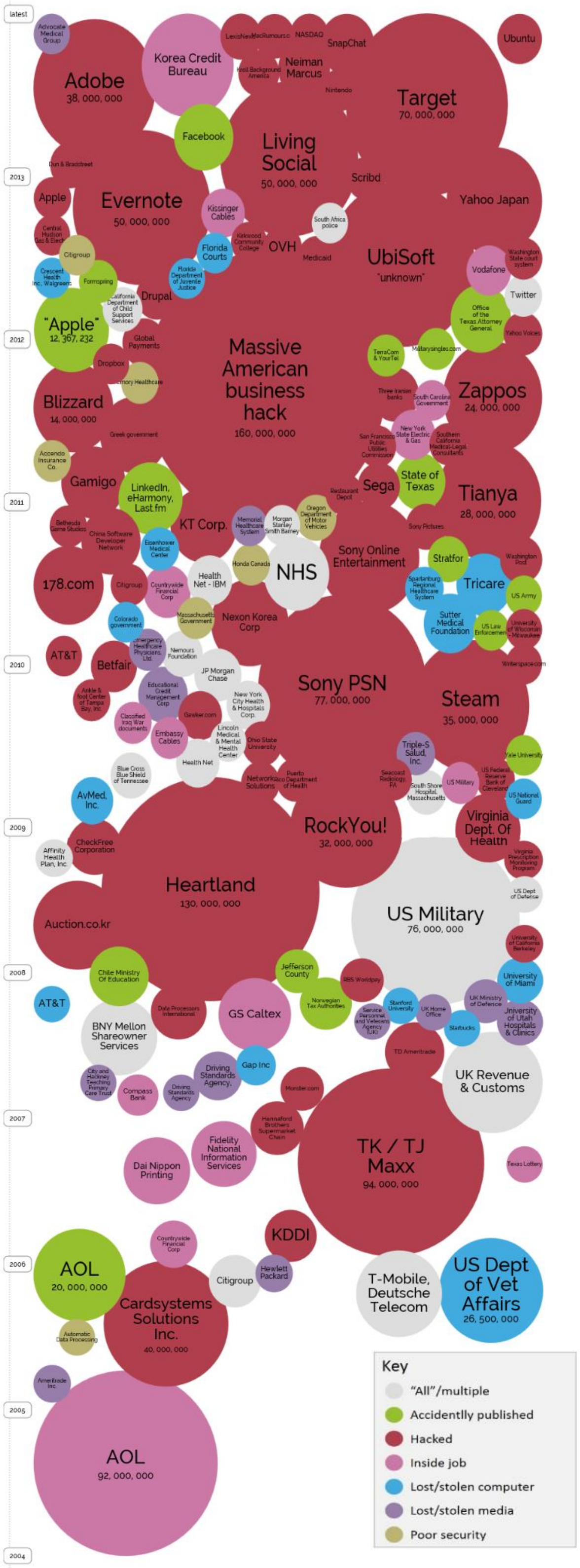
Despite the "good news" verdict on IT security, there's no denying that the threats that IT security frameworks address are becoming both more pernicious and a greater threat to the success of IT-dependent businesses – which is to say, nearly all businesses!

The Figure on the right, sourced from Information is Beautiful, provides a graphic illustration of major data breaches over the past decade. As we follow the progression up the chart, we see (from the number of bubbles associated with each year) that breaches are becoming more common. We see (from the size of the bubbles) that they are affecting more users, as businesses build larger and larger repositories of customer or citizen information. And we see (with the growing predominance of red bubbles, as compared with all other colours) that breaches increasingly result from targeted attacks by hackers, rather than as a result of lost media, accidental data releases or other causes.

This last finding comes as no surprise: larger, richer data assets provide an attractive target for criminals. Data security professionals are better trained and better equipped to deal with incursions – but even still, according to a recent McKinsey & Company report (Risk and responsibility in a hyperconnected world) "Defenders are losing ground to the attackers. Nearly 80 percent of technology executives said that they cannot keep up with attackers' increasing sophistication."

Dell Chief Security Officer John McClurg, in an interview with InsightaaS.com, was even more direct: "It doesn't matter if you are small or large, it's not a matter of **'if'** you are going to be compromised, it's **'when'**." McClurg also explained that in an interconnected world, each business is a potential point of penetration for a supplier or customer – meaning that hackers may target small firms as a means of getting to larger ones, and meaning as well that the "security through obscurity" approach frequently observed within small businesses provides less protection today than it might have in the past.

Figure 5. Data Breaches: 2004-2013

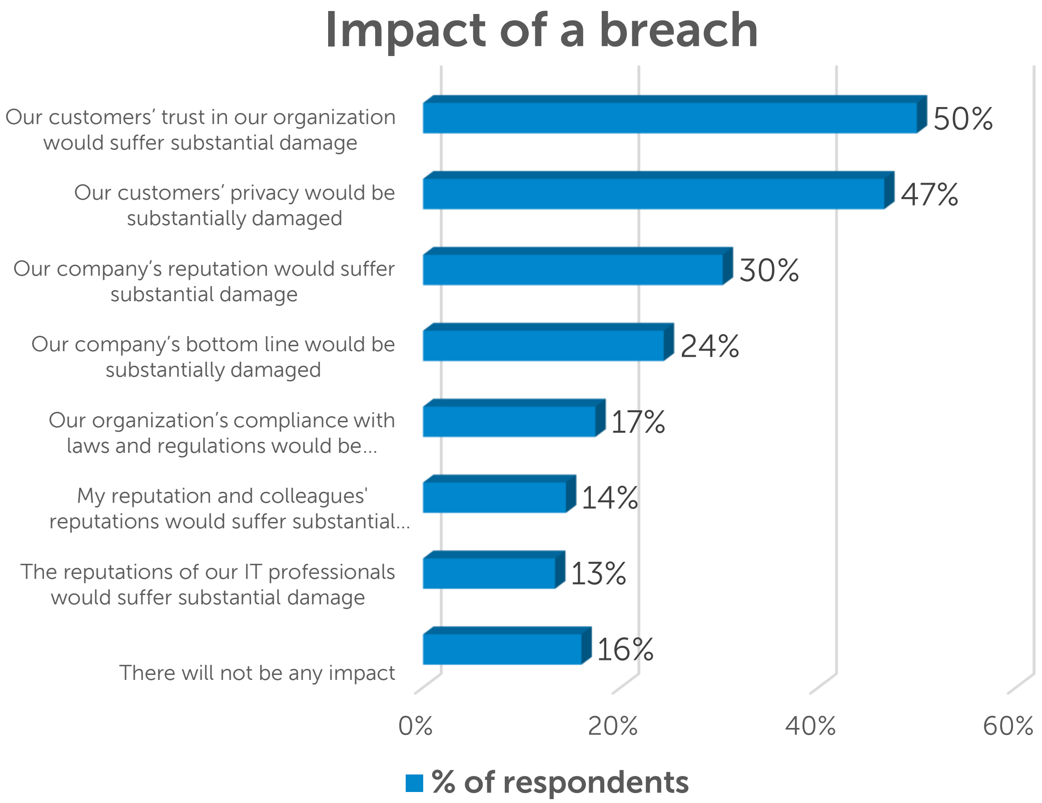


Source: Information is Beautiful

The impact of a breach

In the Techaisle survey of Canadian ITDMs and BDMs, respondents were asked "– what would be the impact on your organization if there was a security/data breach of corporate information?" Responses indicate that the damage would be widespread and substantial. As Figure 6 demonstrates, the most severe consequence of a breach would be damage to customer relationships, but there would also be damage to corporate reputations and profitability, difficulty in meeting regulatory requirements, and personal reputation damage for both business and IT professionals within the firm.

Figure 6. What would be the impact of a security/data breach?

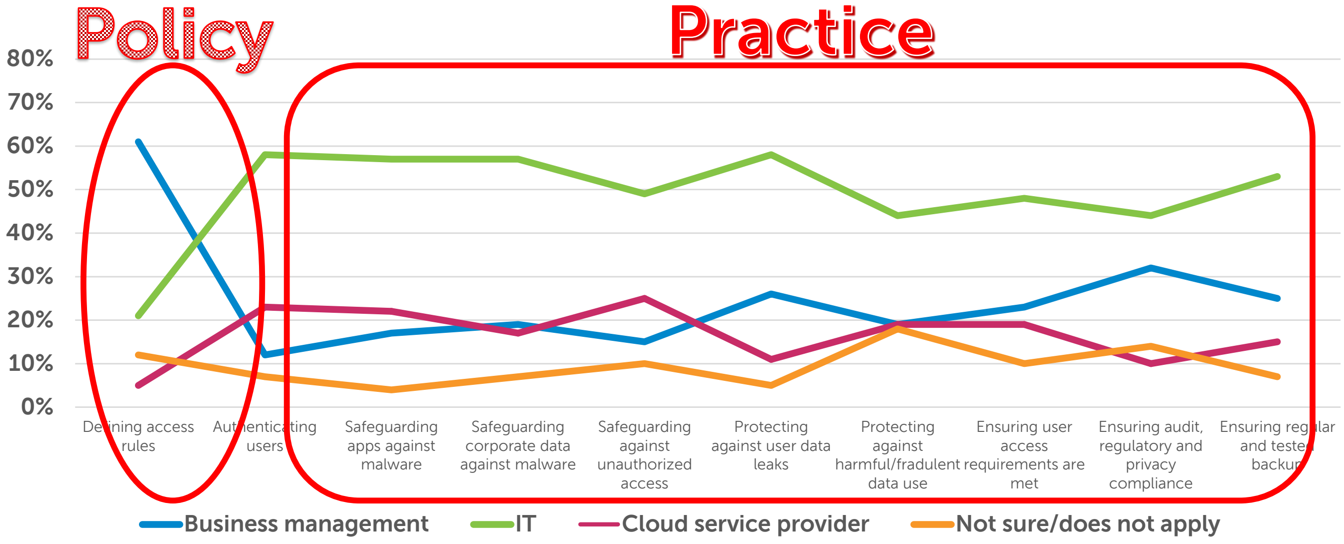


Source: Techaisle survey of 635 Canadian ITDMs and BDMs, December 2013

Management approaches suffer from an important disconnect

Other Techaisle data – from a parallel survey of 820 US-based ITDMs and BDMs – illustrates a potential problem area for security management. Responses to a question asking who – business management, IT, or cloud suppliers – has responsibility for the various steps required to safeguard cloud-based applications and data yield a fascinating insight: there is a significant disconnect between responsibility for security *policy*, which is largely in the hands of business management, and security *practice*, which is the domain of IT professionals. It isn't impossible for this type of relationship to work – but it does require constant and efficient collaboration between the two groups. The importance of effective two-way communications becomes even clearer when we consider the impact that "shadow IT" – sourcing of IT products and services directly by business managers, without the involvement of the IT department – will have on an organization's overall security profile. Will communications between business managers and IT be solid enough to ensure that security practices are applied to shadow resources? Or will the practice falter as business managers make independent use of new systems without IT involvement?

Figure 7. Disconnects in security policy and practice for cloud-based systems



Source: Techaisle survey of 820 US ITDMs and BDMs, December 2013

Netting out the downside of security threats

Scanning what McKinsey calls the "hyperconnected world," we see a troubling combination of threats and potential sources of exposure. Businesses are not only increasingly dependent on IT – they are dependent on increasingly-interconnected systems, which are in turn open to an ever-expanding population of devices and access points. The volumes and value of data contained in these systems continues to grow, which both increases the potential damage associated with a breach, and attracts heightened attention from hackers. Meanwhile, we find a disconnect between security (policy) authority and security (practice) responsibility that creates the potential for poorly-coordinated approaches to security – an uncertainty that is magnified by shadow IT. If we look at the "good news/bad news" associated with security threats, we find that there is very little on the positive side of the ledger: only the fact that with shadow IT, business managers may gain new appreciation for the importance and complexity associated with adequately security new systems. Security may be an enabler of success rather than an anchor on progress – but it is also a critical component of business strategy needed to address a substantial and increasing threat landscape.

Figure 8. On balance: IT security and the downside of security threats

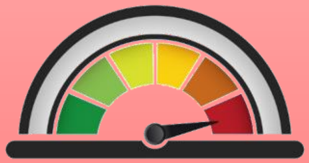
Good News:

- (potentially) Increased business management understanding of security requirements due to involvement with shadow IT

Bad News:

- Increased use of connected systems;
- Increased variety of access points/devices
- Increased data volumes and value
- Increased volume and magnitude of breaches
- Substantial exposure
- Potential for mis-alignment between policy and practice

THE VERDICT:



- *The threat landscape is more pernicious than ever – it is getting ever-thornier – there is a disconnect between responsibility and authority – and the downside is worse than ever before*

IT security options and upside

If there is any real upside in the dark clouds gathering on the threat landscape, it's that security is becoming a more critical component of business (rather than IT) strategy. In fact, McKinsey, in its "Risk and responsibility" report, notes that "Given the cross-functional, high-stakes nature of cybersecurity**,** it is a CEO-level issue, and progress toward cyberresiliency can only be achieved with active engagement from the senior leaders of public and private institutions."

IT security-responsible management, then, can expect senior executive visibility, and should be able to expect – or at least, petition for – senior executive support. With that oversight and endorsement, they will be expected to build an approach that safeguards their organizations, users and data, in a framework that is flexible enough to respond to emerging opportunities and threats. InsightaaS has developed a four-layer model for deploying this type of framework:

1. *Secure the perimeter.* The most important aspect of what Dell's McClurg refers to as the "minimally essential core" of a security strategy is a secure framework. This involves protecting the network and its devices against hacks, intrusions and malware. Firewalls that protect in-transit data are a key secure perimeter technology, as are anti-malware products deployed on client devices and access points.
2. *Secure at-rest data.* The second critical component in the four-layer model is security for at-rest data. The most important element at this layer is encryption technology; as McClurg said in his InsightaaS interview, you want to ensure that any hacker who penetrates the hardened perimeter "gets the bad taste of a heavily encrypted solution." Data loss prevention (DLP) technology that prevents leakage of data resident on mobile devices is an extension of at-rest data security. Another key 'to do' in this category involves separating data into discrete domains, so that hackers accessing one part of a network don't automatically gain access to all network-resident information. This step may well require IT and business to work together to identify and classify different pools of information, which can be assigned varying levels of security and isolation depending on their importance,
3. *Take steps to protect against employee vulnerabilities.* Most security technologies are designed to protect against external threats – but, as the "accidentally published" and "inside job" bubbles on the Information is Beautiful graphic show, employees can be the source of substantial data breaches. Effective access policies (and enforcement of those policies), training and regular awareness campaigns can help protect against inadvertent data leakage. Malfeasance can be more difficult to protect against, though new analytics tools can help highlight patterns that might indicate malicious activities.

John McClurg, VP and Chief Security Officer, Dell Inc.

4. *Apply intelligence widely in the security process.* Hackers actively distribute exploits and information on vulnerabilities, and as a result, the nature of threats continues to evolve. However, there is active information sharing amongst the white hats as well. Security-responsible managers can subscribe to services (such as Dell's SecureWorks CTU Threat Intelligence services) that provide up-to-the-minute intelligence on emerging threats. This kind of insight allows IT managers to align defenses with highest-priority issues – as long as the overall framework is flexible enough to allow extensions from the "minimally essential core" to areas of immediate and specific need.

There is one additional, critical consideration that IT managers must overlay on this four-layer framework: the need to integrate within and across the layers. A hardened perimeter is only as hard as its softest point; to be effective, the 'shields' need to connect/overlap in ways that do not leave vulnerabilities that hackers can exploit. Similarly, data that is tagged as high-priority for encryption needs to be protected on one side from poorly-secured endpoint devices and on the other from employee mistakes or malfeasance.

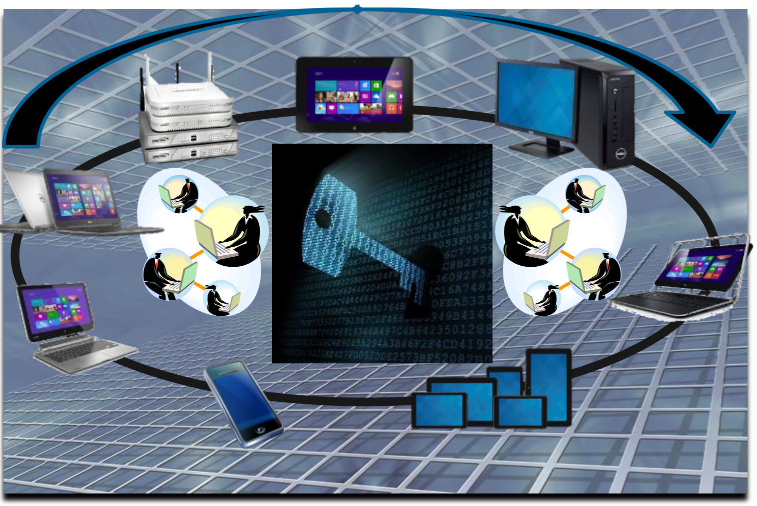
Figure 9. A four-layer approach to establishing an effective security framework

Four layers of cyber defence...

1. Secure the perimeter
2. Secure "at rest" data
3. Take steps to safeguard against employee vulnerabilities
4. Apply intelligence widely in the security process

...with one key overlay:

- *Integration within and across the layers*



Source: InsightaaS.com

Netting out the "good news/bad news" security equation

Neither the four-layer framework nor any other approach to IT security can provide a 'silver bullet' to safeguarding users and corporate information. Effective IT security requires a combination of budget, technology, internal expertise, access to external experts, training, insight, strategy, and a great deal of hard work – and even then, as McClurg pointed out, it's possible that the 'bad guys' will penetrate corporate defenses and cause damage.

On balance, though, managers responsible for IT security have many reasons for optimism. As our final "good news/bad news" graphic illustrates, IT security managers can and should expect to have visibility and support at the highest levels of their organizations. They can deploy technologies that are getting better all of the time – and with the deployment and integration methodologies that suppliers like Dell are introducing, they can get expert guidance on how to arrange 'the shields' to obtain maximum benefit/protection. Processes for managing data and employees are also improving. And perhaps most importantly, the demands on IT to constantly deploy systems required by agile businesses increase every day. True agility is impossible if each new solution is delayed prior to deployment as IT management searches for unique security answers for each new requirement. An effective framework-level approach to IT security isn't just a way to simplify security management – it's a means of enabling a business's ability to respond quickly to competitors and to new market opportunities.

The 'news' isn't all good: attacks on data resources continue to increase, the threats themselves continue to proliferate, with new threat types, played out over varying timeframes (patient and immediate) and through both technologies and staff, seeming to emerge every day; and with the expanding corporate reliance on IT, security failures are increasingly visible and damaging.

On balance, though, the 'needle' is definitely trending upward for IT security. Experience shows that issues that are important to senior management are important to the entire organization – so if McKinsey is right in stating that IT security is a CEO-level issue, IT security staff should expect both increased visibility and increased resources. The supply community continues to improve the breadth, capabilities and integration of their products, and to complement products with advanced services. And IT security managers themselves are increasingly able to move past firewall configuration and malware deployment to addressing issues at the core of business processes – and by doing so, position themselves as contributors to the success and profitability of their businesses.

Figure 10. On balance: IT security is an essential component of success and profitability

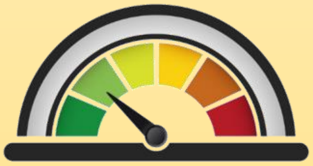
Good News:

- IT security managers can and should expect C-level visibility/support
- Security technologies are improving
- Deployment and integration practices are improving
- Data and employee management processes are improving

Bad News:

- Frequency and severity of attacks on data resources are increasing
- New threat types and timeframes emerging
- Security failures are increasingly visible – and damaging

THE VERDICT:



- *The challenge is real and substantial – but with senior executive visibility and support, better tools and a strong support community, IT security managers are well-positioned to drive success and profitability!*