Aberdeen Group
A Harte-Hanks Company

November 2010

The State of IT (In)Security, and How to Avoid Costs by Investing More

In a study of more than 160 worldwide organizations, Aberdeen found that respondents annually spend an average total of $2,150,000 in IT Security-related activities: $870,000 invested in their IT Security initiatives, plus an additional $1,280,000 in costs related to IT Security incidents that were not avoided in spite of these investments. The total works out to approximately $220 per employee per year, or roughly 0.2% of annual revenue – less than many companies spend on complimentary tea and coffee. Aberdeen's further analysis by company size, however, shows that Large enterprises are investing disproportionately much less than Mid-Size and Small businesses. How should Small and Mid-Size organizations successfully optimize the balance between their annual investments in IT Security initiatives, and the additional financial impact of IT Security-related costs not avoided – the very essence of a risk-based approach?

Context: Current Landscape for IT Security Initiatives

Aberdeen's study of more than 160 worldwide organizations confirms that IT Security remains extremely high in importance, with nearly 9 out of 10 (87%) of all respondents ranking it a 4 or 5 on a scale of 1 (unimportant) to 5 (imperative). The average ranking, across all respondents, is 4.42. This explains in part why primary ownership and accountability for IT Security at 87% of all participating organizations belongs to C-level management. In fact more than three-fourths (76%) of all respondents indicated a year-over-year *increase* in the focus of the senior management team on IT Security-related risks, and the actions taken to manage them. Not surprisingly, such C-level focus brought additional resources to bear as well; two-thirds (66%) of all respondents also indicated a year-over-year increase in their organization's total investments in IT Security initiatives (including all related people, process, and technologies). For another 29%, total expenditures on IT Security initiatives remained the same as the previous year, in spite of current economic conditions – leaving just one organization in twenty whose IT Security budgets decreased. Moreover, 7 out of 10 (69%) respondents reported a year-over-year increase in general awareness of IT Security-related policies among their employees – positive evidence that companies are also taking steps internally to get the word out about security and risk.

Why is this the case? The simple explanation is that IT Security risks are abundant, and equal opportunity in nature; in the past 12 months, 94% of all respondents experienced at least one IT Security-related incident. These range from the more common (e.g., *malware*, *non-criminal misuse of company systems*, *loss or theft of IT assets*, *insider misuse of access privileges*) to the less

Sector Insight

Aberdeen's Sector Insights provide analysis and strategic perspective of primary research results by company size, geography or industry

Research Demographics

Between September and October 2010, Aberdeen examined more than 160 enterprises; respondents had the following demographics:

√ **Job title:** C-level management (27%); Vice President (8%); Director (15%); Manager (24%); Staff / Consultant (23%)

√ **Functional responsibility:** the largest segment was IT (56%)

√ **Industry:** the largest segments included financial services (17%); government / aerospace / defense (14%); telecommunications (11%); and education (9%)

√ **Geography:** Americas (55%), Europe / Middle East / Africa (29%); Asia / Pacific (16%)

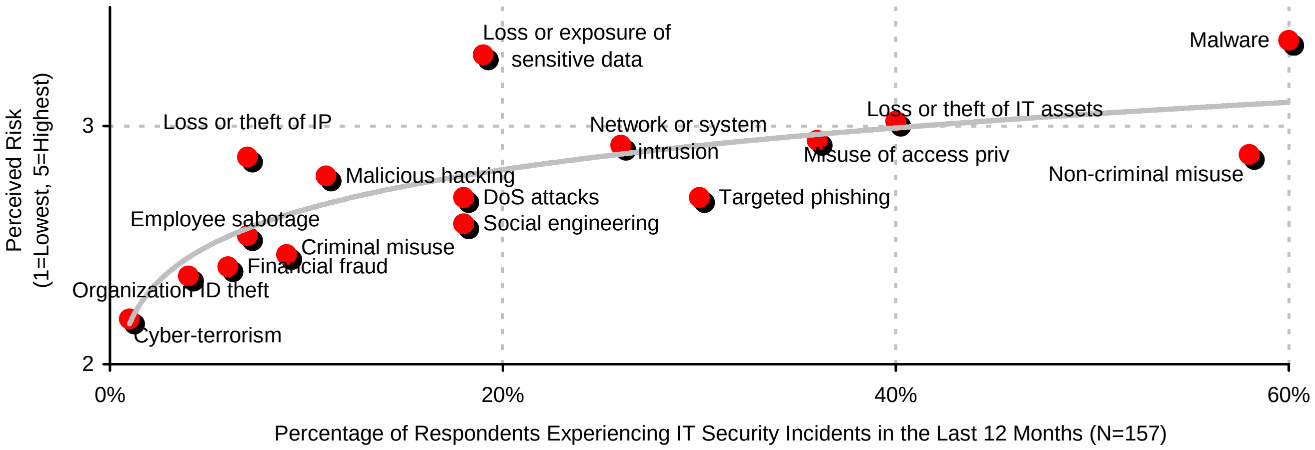
√ **Company size:** Large enterprise (20%); Mid-Size enterprise (39%); Small enterprise (41%)

common but potentially crippling (e.g., *loss or theft of intellectual property*, *employee sabotage*), with a diverse array of IT Security-related vulnerabilities and threats in between. Over the last 12 months, the average number of IT Security-related incidents (of any type) experienced by participants in Aberdeen's study was 10.7.

IT Security Risk: Reality vs. Perception

Interestingly, the *perception* of IT Security risk is only moderately correlated with the number of IT Security incidents *actually experienced* in the last 12 months (Figure 1). Respondents generally ranked their current assessment of risk from a wide variety of IT Security-related incidents to be on the low side, i.e., less than 3 on a scale of 1 (lowest) to 5 (highest). The risks that are perceived to be the highest include **malware**, **loss or exposure of sensitive data**, **loss or theft of IT assets**, **loss or theft of intellectual property**, **misuse of access privileges** (by insiders), and **network or system intrusion** and **malicious hacking** (by outsiders).

Figure 1: IT Security-related Incidents Experienced in the Last 12 Months, versus Perceived Risk



Source: Aberdeen Group, November 2010

The Consequences of IT Security Incidents

The consequences of actual IT Security-related incidents are as varied as the types of incidents themselves; the most commonly noted consequences were:

- Loss of end-user productivity (70% of all respondents)
- Unplanned downtime (64%)
- Internal disciplinary process (51%)
- Employee termination (36%)
- Loss or exposure of sensitive data (32%)
- Damage to brand or reputation (20%)

For the participants in Aberdeen's study, the average financial impact per actual IT Security-related incident was estimated at $120,000. Note that this figure represents a *blended* amount for *all* of the incident types listed in Figure 1. Previous Aberdeen research has found, for example, that the average financial impact for a data loss or data exposure incident ranges between $500,000 and $640,000; for remediating an application security vulnerability, it was $300,000. For the purposes of this Sector Insight, Aberdeen's analysis will use the blended figure of $120,000.

Looking at the consequences of IT Security incidents from a different perspective, for those organizations that experienced financial losses in the last 12-month reporting period the average amount estimated to be attributable to IT Security incidents was 4.6%.

Quantifying Business Value: Cost Savings, Cost Avoidance

For the purposes of assessing the business value of an organization's annual investments in IT Security, Aberdeen uses the following simple equation:

$$\frac{\text{(Total Cost of IT Security-related Incidents Avoided)}}{\text{(Total Annual Cost of IT Security Initiatives)} + \text{(Total Cost of IT Security-related Incidents Not Avoided)}}$$

The denominator includes the total annual cost for the organization's IT Security initiatives; also in the denominator, however, are the total costs from IT Security incidents that were *not* avoided in the last 12 months, *in spite of* the investments that have been made. In the numerator are the best estimates for the total costs of IT Security-related incidents that *were* avoided in the last 12 months as a result of the organization's investments – these may be difficult to come by, and imprecise at best. For this reason, the most general way to think about this simple analysis is that any investments in technologies and services that lower the total cost of the initiative (*efficiency*) and cause a greater shift from the denominator to the numerator in terms of incidents avoided (*effectiveness*) will have a strongly positive impact on the overall return on annual investment.

Given an average of 10.7 incidents experienced in the last 12 months, and an average financial impact of $120,000 per incident, the total cost of IT Security-related incidents not avoided is $1,280,000 per year, in spite of an average expenditure of $870,000 on IT Security initiatives. That is, the average respondent in Aberdeen's study invests a total of $2,150,000 per year in IT Security-related activities. This total works out to approximately $220 per employee per year, or roughly 0.2% of annual revenue. Many companies spend more than this on complimentary tea and coffee.

Notice the *ratio* of the total cost of IT Security initiatives, however, versus the total cost of IT Security-related incidents not avoided. For every $100 invested to reduce or prevent incidents from happening, companies are still spending an additional $147 as a result of incidents that happened anyway. There may be no such thing as "perfect" security – that is, one could invest an infinite amount to prevent incidents from happening, and yet an incident may still happen – but is this the optimal balance? Aberdeen's analysis by size of company, below, provides some

Why We Don't Invest: People and Process, Not Technology

Excluding cost-related factors, **people** and **process** issues are significantly greater *inhibitors* to current investments in IT Security than those related to available **technologies**. Leading examples include:

- **People:** staff lack the necessary bandwidth (e.g. time and resources); staff lack the necessary skill sets and experience; responsibility and ownership are dispersed among different groups
- **Process:** complexity and diversity of the current computing environment; resistance to changing existing practices; perception that security initiatives will adversely impact existing business processes; lack of consistent policies

Among cost-related factors, **cost to acquire** is of higher concern than **cost to deploy** or **cost to manage**. Analysis almost always demonstrates that the latter have a greater impact on the total cost of ownership over a period of time, but – as we have all experienced – enterprise budgets are often established and approved based on what can or cannot be spent right now, rather than on what will end up being spent over time.

Market Trends: Current Capabilities and Technologies Used to Detect and Prevent IT Security Incidents

The state of IT Security is in truth a state of insecurity; among all respondents, only 9% are "completely confident" in their ability to detect IT Security-related incidents. On average, companies rate their confidence at a very slightly positive 3.2 on a scale of 1 (not confident at all) to 5 (completely confident). Not surprisingly, the most common means of detection are *proactive* – **IT Security products and services, scanning and testing**, and **internal audits** – as opposed to being informed by customers, business partners, law enforcement, or public media.

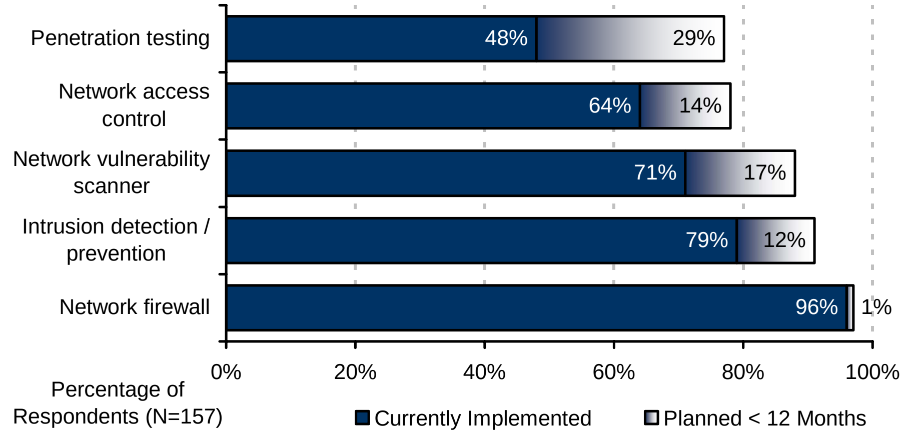
Current, Planned Use of Selected IT Security Technologies

Aberdeen asked respondents about their *current* use of a wide range of IT Security technologies, as well as their *planned* use of those technologies in the next 12 months. For convenience, findings are presented for selected IT Security technologies in the following high-level categories: **network security**, **endpoint security**, **application security**, **identity and access management technologies**, and **data security**.

A majority of companies have invested in core IT Security technologies for securing their **networks** (Figure 3). Nearly all (96%) have deployed *network firewalls*, and 4 out of 5 (79%) have deployed *intrusion detection / prevention* solutions to defend their network infrastructures. In addition, current deployments of *network vulnerability scanning* (71%) and *penetration testing* (48%) provide evidence of a generally proactive approach to managing and security enterprise networks. Two-thirds (64%) of respondents have also implemented *network access control*; see Aberdeen's Research Brief Five Key

Capabilities for Gaining Visibility and Control over Your Network Devices, Endpoints and End-Users (September 2010), and look for the upcoming benchmark study *The Zen of Network Access: First There Was a Border, Then There Was No Border, Then There Was* (planned December 2010) for additional insights.

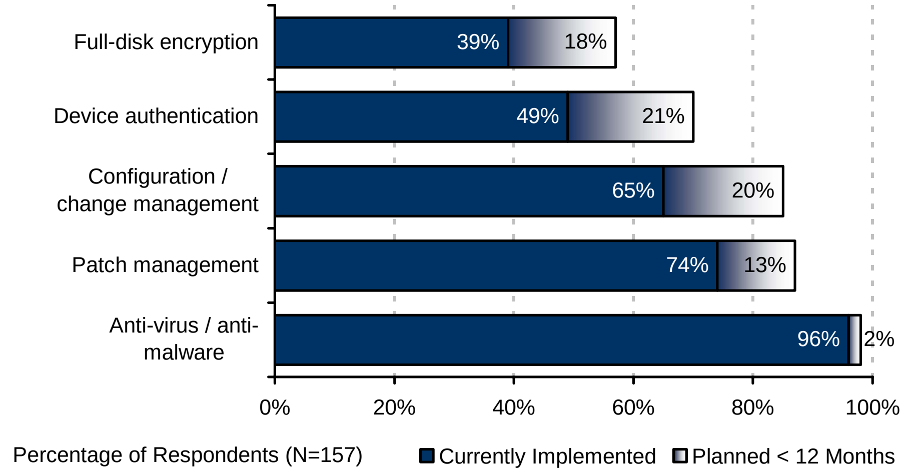
Figure 3: Network Security Technologies (current, planned)



Source: Aberdeen Group, November 2010

Most companies have also invested in core IT Security technologies for securing and managing their **endpoints** (Figure 4). Nearly all (96%) have deployed *anti-virus / anti-malware* solutions, and a majority have deployed *patch management* (74%) and *configuration and change management* (65%) – more evidence of a generally proactive approach. Aberdeen's research on *What's Protecting Your Endpoints?* (October 2010), Laptop Lost or Stolen? Five Questions to Ask and Answer (February 2010), and Full-Disk Encryption On the Rise (September 2009) provides additional details and insights in these areas.

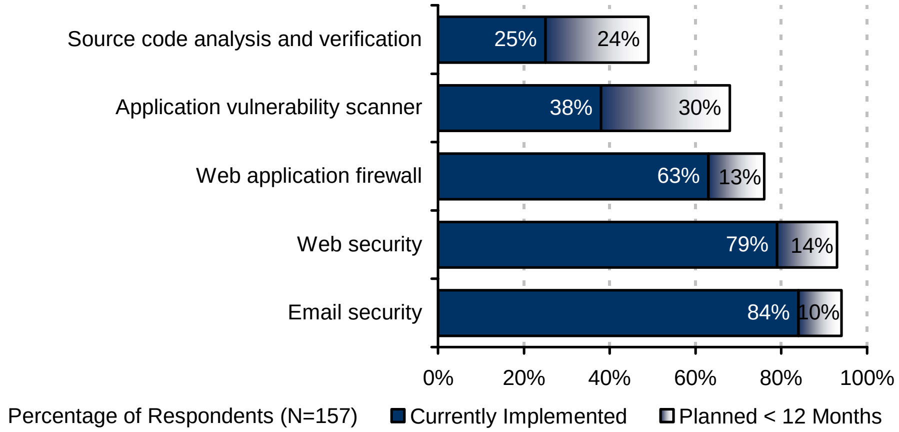
Figure 4: Endpoint Security Technologies (current, planned)



Source: Aberdeen Group, November 2010

A majority of companies have invested to protect themselves against vulnerabilities in their email, web access and web-based applications (Figure 5). *Email security* (84%) and *web security* (79%) are well-established as baseline technologies, and *web application firewalls* have been deployed by nearly two-thirds (63%) of all respondents. For additional insights on technologies and best practices in these areas – and **application security** in general – see Aberdeen's research on *Email Security in the Cloud* (April 2010), *Web Security in the Cloud* (May 2010), *Securing Your Applications: Three Ways to Play* (August 2010), *Application Scanning and Penetration Testing: Find and Fix (Later)* (September 2010) and *Web Application Firewalls: Defend and Defer* (October 2010).

Figure 5: Application Security Technologies (current, planned)

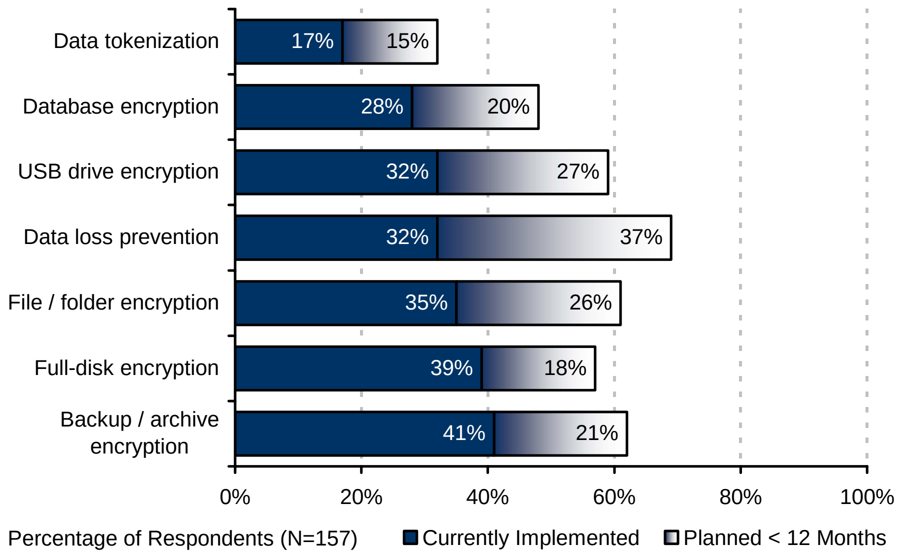


Source: Aberdeen Group, November 2010

Investments in technologies to manage **identities and access** are slightly

Finally, across all respondents investments are seen to be lagging in the area of protecting sensitive **data** (Figure 7), which although not positive is at least consistent with the findings regarding perceived risk presented in Figure 1. Additional insights in these areas can be found in Aberdeen's research on *Protecting Data in Databases vs. Applications: Better Security and Compliance at Lower Cost* (April 2010), *Full-Disk Encryption On the Rise* (September 2009), *Content Aware: The 2010 Data Loss Prevention Report* (June 2010), *Putting the P in DLP (July 2010)*, and *Avoiding a Kick to the Head: The Value of Tokenization for Protecting Cardholder Data* (January 2010).

Figure 7: Data Security Technologies (current, planned)



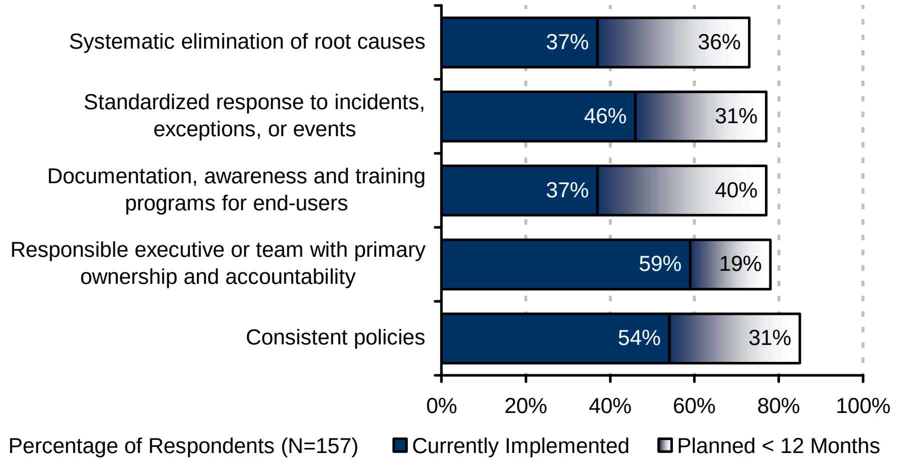
Source: Aberdeen Group, November 2010

Current Capabilities: Process, Organization, Knowledge Management, Performance Management

In addition to asking respondents about their current and planned use of IT Security technologies, Aberdeen investigated current capabilities related to **process** (the approaches taken to execute daily operations), **organization** (corporate focus and collaboration among stakeholders) **knowledge management** (putting business intelligence in context and exposing it to relevant stakeholders), and **performance management** (measurement of results to improve the business). In general, current capabilities reveal the relative immaturity of process, organization, knowledge management, and performance management for the average respondent.

In just more than half of all respondents, the presence of an executive or team with *primary ownership and responsibility* for IT Security initiatives (59%) – the time-honored “one throat to choke” principle – and the existence of *consistent policies* for IT Security (54%) may mask the underlying lack of critical capabilities in other areas (Figure 8). For example, less than half (46%) of all respondents have a *standardized response* for IT Security-related incidents, exceptions or events, and fewer than 2 out of 5 (37%) make a systematic effort to *eliminate root causes*. These are the conditions that tend to keep companies mired in manually intensive activities and individual heroics, in which the work gets done but at greater time and cost.

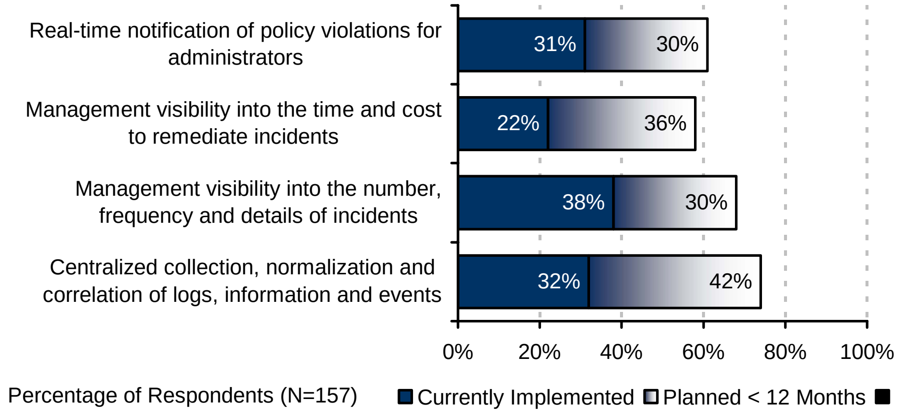
Figure 8: Current Capabilities – Process, Organization



Source: Aberdeen Group, November 2010

Fewer than one-third (32%) of companies have centralized IT Security-related information and events (Figure 9), which leads to less than 2 out of 5 (38%) companies indicating that they have management visibility into the number, frequency and details of IT Security incidents, and just 1 out of 5 (22%) indicating that they have management visibility into the time and cost of remediation. Think back again to the ratio of total investments in IT Security initiatives versus the total impact of IT Security-related incidents not avoided – an additional $147 in additional costs, for every $100 invested – and it is easy to support the conclusion that people and process, not technologies, are the most attractive targets for incremental improvement.

Figure 9: Current Capabilities – Knowledge, Performance



Source: Aberdeen Group, November 2010

Drilldown: Analysis by Company Size

To gain additional insights into the state of IT Security, Aberdeen analyzed the responses as a function of company size, based on the following sector definitions: 61 respondents from **Small** enterprises ($50M or less revenue in the most recent 12-month reporting period); 60 respondents from **Mid-Size** companies (between $50M and $1B); and 29 respondents from **Large** organizations ($1B or higher).

Compared to Mid-Size and Small businesses, Large organizations rank IT Security slightly higher in importance. Focus of senior management on IT Security, total expenditures and IT Security, and general awareness of IT Security policies among all employees is also higher for Large organizations on a year-over-year basis.

Yet Small and Mid-Size enterprises are investing disproportionately more than Large enterprises, as summarized in Table 1:

- The total annual investment in IT Security is $140 per employee for Large, $590 per employee for Mid-size, and $1200 per employee for Small.
- The total annual investment in IT Security is 0.1% of annual revenue for Large, 0.6% of annual revenue for Mid-Size, and 3.8% of annual revenue for Small. For the Small enterprise in particular, this is a material amount; what small business would not be interested to increase its bottom line by nearly 4%?
- For every $100 invested annually to reduce or prevent IT Security-related incidents from happening, the additional annual expense as a result of incidents that happened anyway is $64 for Large, $200 for Mid-Size, and $357 for Small.

Sector Definitions

For the purposes of this Sector Insight, the following terms are defined by an organization's revenue in the most recent 12-month reporting period:

√ **Large:** $1B or higher

√ **Mid-Size:** less than $1B and more than $50M

√ **Small:** $50M or lower

Table 1: Comparing the Business Value of Annual Investments in IT Security, by Company Size

Averages for Participants in This Study	All Respondents	Large (>$1B)	Mid-Size ($50M-$1B)	Small (<$50M)
Number of IT Security-related incidents experienced in the last 12 months	10.7	16.5	10.8	6.2
Total annual impact of IT Security incidents	$1,280,000	$1,980,000	$1,300,000	$750,000
Total annual cost of IT Security-related initiatives (includes all related costs for people, process and technologies)	$870,000	$3,080,000	$650,000	$210,000
Total annual investment in IT Security	$2,150,000	$5,060,000	$1,950,000	$960,000
Ratio of Total Annual Costs Not Avoided to Total Annual Cost of IT Security Initiative	1.47	0.64	2.00	3.57
% of annual revenue	0.2%	0.1%	0.6%	3.8%
$ impact per employee per year	$220	$140	$590	$1,200

Note: for participants in this study, the average total financial impact for a single IT Security-related incident was $120K
Source: Aberdeen Group, November 2010

Optimization of the tradeoffs between annual investments in IT Security initiatives, versus the additional costs of IT Security-related incidents not avoided, is the very essence of a risk-based approach. Aberdeen's analysis shows that Large organizations are currently winning the game in this regard.

People, Process

Regardless of size, all companies perceive risks from *malware* and *data loss or data exposure* to be high (Table 2); Large enterprises have the widest view.

Table 2: IT Security-related Risks Perceived to be Above Average

Perceived Risk Above 3.0	Large	Mid-Size	Small
Data loss or exposure	X	X	X
Malware infection	X	X	X
Loss or theft of IT assets	X		
Network / system intrusion	X		
Misuse of access privileges	X	X	
Criminal misuse of systems	X		
Malicious hacking	X		
Targeted phishing	X		
Social engineering	X		

Source: Aberdeen Group, November 2010

Current capabilities that correlate strongly with company size include:

- Consistent policies for IT security
- Standardized response to security-related incidents, exceptions, or events
- Documentation, awareness and training programs for end-users around IT security
- Responsible executive or team with primary ownership and accountability for IT security

In Small enterprises, the CEO is 3-times more likely to own IT Security than in Large enterprises; Large enterprises are 3-times more likely than Small enterprises to have a dedicated CSO or CISO. Claiming IT Security as one of the chief executive's many responsibilities, as opposed to the security executive's primary responsibility, is arguably a cornerstone for all of the other key differences between Large, Mid-Size and Small organizations identified in this analysis.

Technologies

Current use of technologies that correlate with company size include proactive scanning and testing at the network level (*network vulnerability*

Fast Facts

Consistent policies for IT Security

√ Large enterprise 76%

√ Mid-Size enterprise 49%

√ Small enterprise 48%

Standardized response to security-related incidents, exceptions, or events

√ Large enterprise 72%

√ Mid-Size enterprise 46%

√ Small enterprise 31%

Documentation, awareness and training programs for end-users around IT security

√ Large enterprise 66%

√ Mid-Size enterprise 33%

√ Small enterprise 26%

scanners, *intrusion detection / prevention*, *penetration testing*), proactive management and security at the endpoints (*patch management*, *configuration and change management*, *endpoint encryption*), stronger assurance of user identities (*strong user authentication*, e.g., *one-time passwords*, *smart cards*, *biometrics*), and increased visibility through aggregated, correlated information and events (*security information and event management*). The key takeaway is that baseline technologies such as network firewalls, anti-virus / anti-malware, email security and web security are essential, but by themselves these solutions do not differentiate leaders from laggards.

Summary and Recommendations

Across all respondents, expectations for the state of IT Security over the next 12-24 months all point to greater risk: the number of incidents, the probability of experiencing incidents, and the average financial Impact of actual incidents are all expected to increase. In addition, expectations are for still greater pressures from requirements for regulatory compliance. As a result, higher total investments in IT Security are also expected as part of the average organization's attempt to keep up.

Aberdeen's analysis of findings by company size showed that compared to Large enterprises, Small and Mid-Size enterprises have:

- The same *motivations* for investments in IT Security
- Similar experiences in terms of the types of IT Security-related incidents actually *experienced*
- Similar experiences in terms of the *consequences* and average *costs* from IT Security-related incidents actually experienced

Yet on a normalized basis, the expenditures being made by Small business are significantly higher than those being made by Large organizations:

- >30-times more in terms of percentage of annual revenue
- >8-times more in terms of total financial impact per employee

Small and Mid-Size enterprises are making substantial investments in IT Security, but they need to reverse the ratio between their annual investments in IT Security initiatives and the additional "costs not avoided" as a result of actual security-related incidents that are experienced in spite of these investments. The core question is, is *ignoring* risk (which is the same as *accepting* it) – and paying more for it later – your deliberate choice? Aberdeen's research indicates that Large organizations are successfully avoiding costs by investing more – math which will hold true so long as the total financial impact of incidents not avoided remains high relative to the total cost of implementing consistent policies and security controls.

Across all respondents, current use of IT Security technologies shows a focus on networks, endpoints, applications, identities and data – roughly in that order. And although current use of several IT Security technologies are correlated with company size, the real takeaway from Aberdeen's analysis is

Fast Facts

Penetration testing

√ Large enterprise 73%

√ Mid-Size enterprise 52%

√ Small enterprise 36%

Patch management

√ Large enterprise 96%

√ Mid-Size enterprise 77%

√ Small enterprise 64%

Configuration / change mgmt

√ Large enterprise 93%

√ Mid-Size enterprise 65%

√ Small enterprise 52%

Strong user authentication

√ Large enterprise 57%

√ Mid-Size enterprise 42%

√ Small enterprise 36%

Security information and event management

√ Large enterprise 66%

√ Mid-Size enterprise 45%

√ Small enterprise 40%

the powerful impact of clear ownership, focus, disciplined processes, and a proactive, risk-based approach.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research

The Zen of Network Access: First There Was a Border, Then There Was No Border, Then There Was (planned December 2010)

Web Application Firewalls: Defend and Defer (October 2010)

Application Scanning and Penetration Testing: Find and Fix (Later) (September 2010)

Five Key Capabilities for Gaining Visibility and Control over Your Network Devices, Endpoints and End-Users (September 2010)

Securing Your Applications: Three Ways to Play (August 2010)

Putting the P in DLP (July 2010)

Content Aware: The 2010 Data Loss Prevention Report (June 2010)

Web Security in the Cloud (May 2010)

Email Security in the Cloud (April 2010)

Access Management: Efficiency, Confidence and Control (April 2010)

Protecting Data in Databases vs. Applications: Better Security and Compliance at Lower Cost (April 2010)

Laptop Lost or Stolen? Five Questions to Ask and Answer (February 2010)

IT Security: Balancing Enterprise Risk and Reward; January 2010

Avoiding a Kick to the Head: The Value of Tokenization for Protecting Cardholder Data (January 2010)

Full-Disk Encryption On the Rise (September 2009)

One-Time Passwords for Two-Factor Authentication (January 2009)

Managing Privileged Users (April 2008)

Author: Derek E. Brink, Vice President and Research Fellow, IT Security (Derek.Brink@aberdeen.com)

Since 1988, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.2 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen plays a key role of putting content in context for the global direct and targeted marketing company. Aberdeen's analytical and independent view of the "customer optimization" process of Harte-Hanks (Information – Opportunity – Insight – Engagement – Interaction) extends the client value and accentuates the strategic role Harte-Hanks brings to the market. For additional information, visit Aberdeen http://www.aberdeen.com or call (617) 723-7890, or to learn more about Harte-Hanks, call (800) 456-9748 or go to http://www.harte-hanks.com