State of Enterprise Security

2010

symantec™

State of Enterprise Security 2010

Table of Contents

Executive summary

Enterprise Security is Difficult

Enterprise security is the classic "caught between a rock and a hard place" scenario.

On one hand, the attacks are frequent and often quite effective. The losses mount quickly -- $2.8 million annually for large enterprises. Organizations face lost productivity, lost revenue, and – worst of all – a loss of customer trust.
On the other hand, providing enterprise security is excruciatingly difficult. Even with massive staffs (230 or more for large enterprises), enterprises feel understaffed. And new data center initiatives – such as cloud computing and virtualization – make the job of providing enterprise security more difficult with each passing day.

Yet despite these difficulties, the **Symantec State of Enterprise Security Report 2010** shows organizations are in constant alert and highlights simple steps IT professionals can take to win the security battle.

Methodology

Applied Research fielded the survey by telephone in January of 2010. The respondents came from three groups:

- Small enterprise (500 – 999 employees)
- Mid-sized enterprises (1,000 – 4,999 employees)
- Large enterprises (5,000+ employees)

The survey respondents came from a wide variety of industries and included a mix of CIOs, CISOs, and senior IT management. Geographically, the study reached 2,100 respondents in 27 countries. The confidence level is 99 percent +/- 2.81 percent.

EMEA	
UK	100
Nordics	100
Germany	75
France	75
Italy	50
Spain	50
Russia	50
Middle East	50
Netherlands	50
Belgium	50
Poland	50

North America	
United States	300
Canada	100

Latin America	
Brazil	73
Mexico	51
Argentina	15
Colombia	11

APJ	
Australia	125
Japan	100
China	100
India	100
Malaysia	100
Singapore	100
New Zealand	75
South Korea	50
Taiwan	50
Hong Kong	50

Finding 1: Enterprise security is IT's top concern

If there is one issue that keeps IT managers up at night it is security. In fact, 42 percent of organizations ranked cyber security as their top risk, beating out such notables as traditional crime, natural disasters, and terrorism.

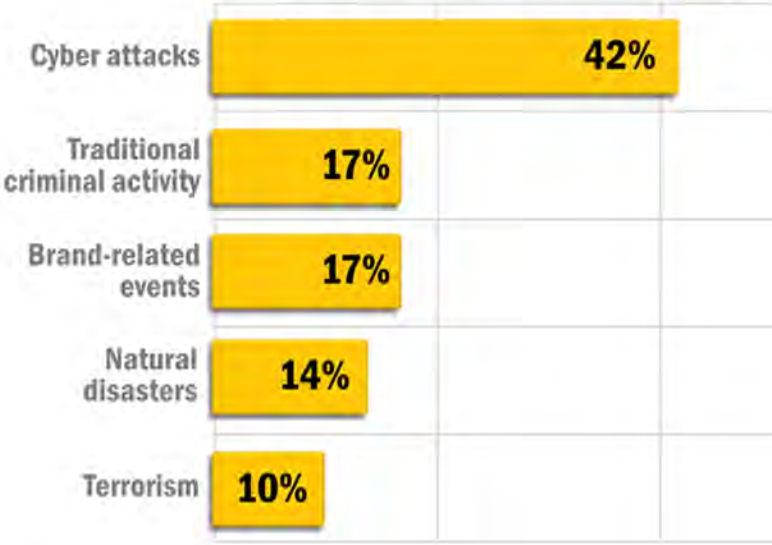
According to a MIS director at a mid-size enterprise, "Enterprise security is the most crucial aspect of running a successful IT infrastructure in any organization."

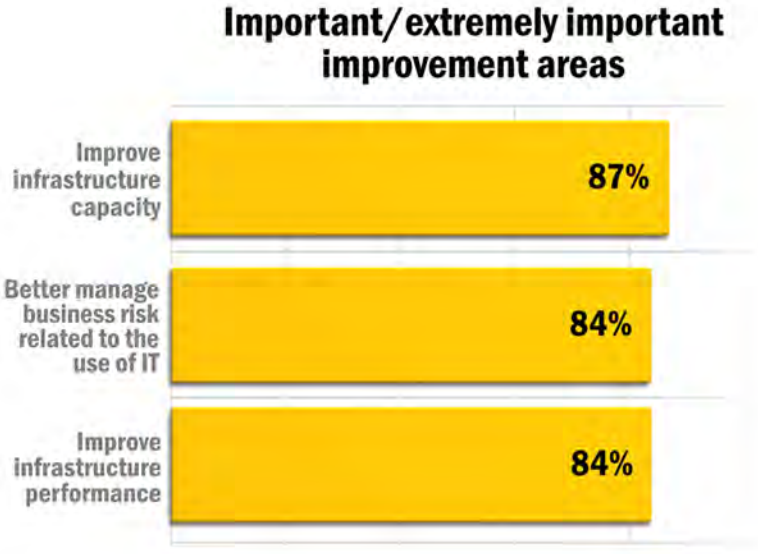
Reflecting that perception, organizations are intently focused on enterprise security. On average, IT assigns 120 staffers to security and IT compliance. In large enterprises the number is even higher – 232.

Furthermore, "better manage business risk of IT" was the second most highly rated goal for IT in our study, right behind "improve infrastructure capacity" Eighty-seven percent rated it "somewhat or absolutely important".

Finally, nearly all (94 percent) expect to implement changes to their cyber security efforts in 2010, with almost half (48 percent) forecasting major changes.

Most significant risks




Important/extremely important improvement areas
Improve infrastructure capacity
87%
Better manage business risk related to the use of IT
84%
Improve infrastructure performance
84%

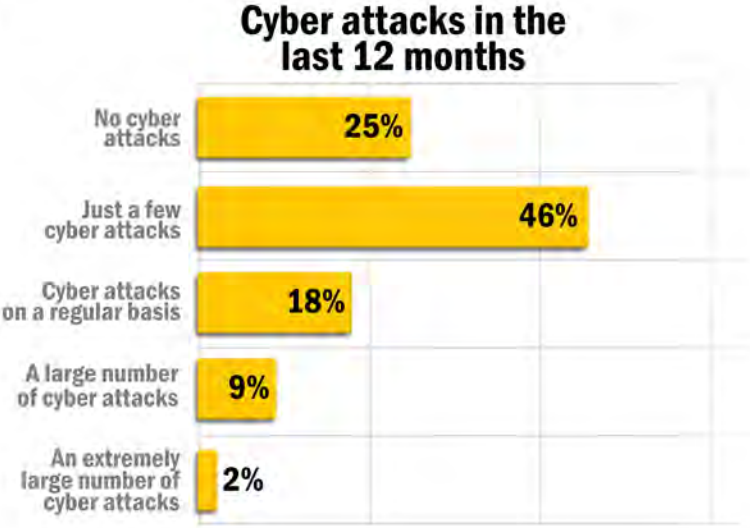
Finding 2: Enterprises experiencing frequent attacks

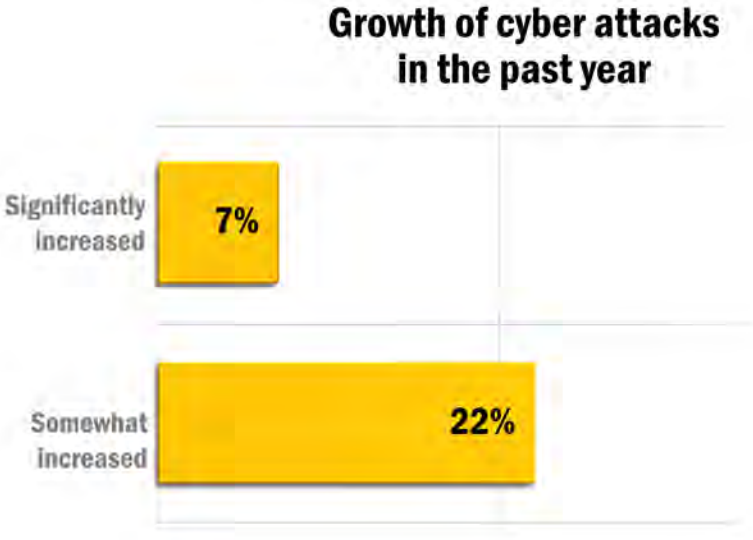
It is easy to see why IT is so focused on security when you consider the frequency of attacks. First, the study found that 75 percent of all enterprises have experienced cyber attacks in the past 12 months. Forty-one percent said these attacks were "somewhat/highly effective."

It is getting worse: When asked about specific types of attacks, 57 percent reported somewhat to extremely fast growth, with "external malicious attacks" the fastest growing type.

Describing the high numbers of attacks on his organization, a director of IT in a 35,000 person manufacturing company states, "We experience about eight or nine attacks a week on average."

According to an IT project manager at a mid-sized federal agency, "You can sit and watch our monitors and see people try to attack us." A MIS director at a mid-size enterprise added, "Every day we see new viruses, new spyware and new backdoors. It is beyond crazy."




Growth of cyber attacks in the past year
Significantly increased
7%
Somewhat increased
22%

Finding 3: Costs of cyber attacks are high

There are real and substantial costs to enterprise IT security breaches. First, the study found that a full 100 percent of the enterprises surveyed had experienced cyber losses in 2009. The most common losses were:

- Theft of customer personally-identifiable information
- Downtime of environment
- Theft of intellectual property
- Theft of customer credit card information

These are critical losses, and led to serious costs to the enterprise in 92 percent of the cases. The most common costs were:

- Lost productivity
- Lost revenue
- Loss of customer trust

The study probed further in an effort to quantify these costs. When pressed, enterprises reported an average combined cost of $2 million annually. For the large enterprises the cost was especially high – almost $2.8 million annually.

One IT operations manager for a 1500 employee auto dealership consortium talks about the cost of losing confidential customer information: "If we lose confidential information, such as social security numbers or credit cards, we're liable. We estimate that it costs us $11,000 a name if there is a compromise in security."

Some costs are harder to quantify, but no less severe. He continues, "The costs of cyber attacks are financial, brand, stock price and a lot of other things as well. But the biggest cost is a ruined reputation. Who wants to do business with a company that cannot protect their customers' information?"

An IT director in a 35,000 person manufacturing company agrees, "Aside from actually losing information you also have public repercussions. If your Web site gets defaced, and it is covered by the media, then your public reputation can suffer."

Finding 4: Security becoming more difficult

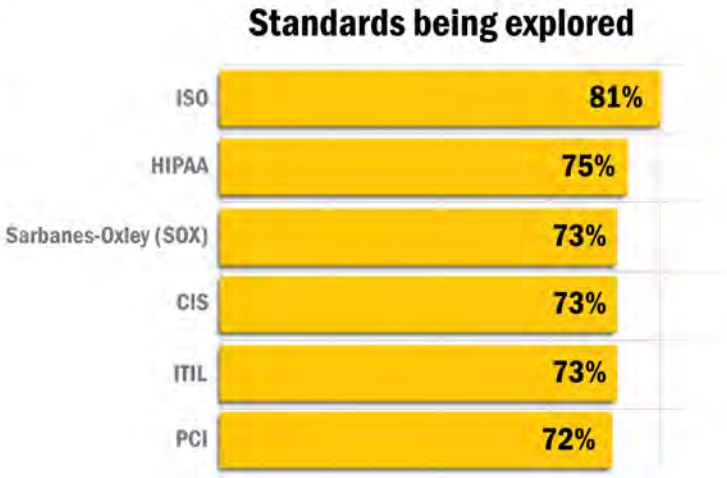
Organizations have their hands full with the high frequency of attacks and staggering losses. Unfortunately, data center realities make it even harder for IT to secure the enterprise.

First, enterprise security is understaffed. The most impacted areas are:

- Security systems management
- Data loss prevention
- Network security
- Endpoint security

This is bad enough, but these security staffing woes come at precisely the wrong time; just as IT is rolling out initiatives that make providing security more difficult. The initiatives that IT rated most problematic from a security standpoint are:

- Infrastructure-as-a-Service
- Platform-as-a-Service
- Server virtualization
- Endpoint virtualization
- Software-as-a-Service



So, two of the hottest new technologies – cloud computing and virtualization – are also the technologies most apt to make security staff's jobs more difficult.

Finally, enterprises are buried with IT compliance efforts. The study found that enterprises are currently exploring a staggering 19 separate IT standards or frameworks and are actually currently using eight of them. The top frameworks/standards mentioned were:

- ISO
- HIPAA
- Sarbanes-Oxley
- CIS
- PCI DSS
- ITIL

Recommendations

So, what can global enterprises do to mitigate cyber risk? It turns out that there are simple measures IT can take that are highly effective.

Protect the infrastructure
Organizations need to protect their infrastructure by securing their endpoints, messaging and Web environments. In addition, defending critical internal servers and implementing the ability to backup and recover data should be priorities. Organizations also need the visibility and security intelligence to respond to threats rapidly.

Protect the information
IT administrators should protect information proactively by taking an information-centric approach to protect both information and interactions. Taking a content-aware approach to protecting information is key in knowing where sensitive information resides, who has access, and how it is coming in or leaving your organization.

Develop and enforce IT policies
Organizations need to develop and enforce IT policies and automate their compliance processes. By prioritizing risks and defining policies that span across all locations, customers can enforce policies through built-in automation and workflow and not only identify threats but remediate incidents as they occur or anticipate them before they happen.

Manage systems
Organizations need to manage systems by implementing secure operating environments, distributing and enforcing patch levels, automating processes to streamline efficiency, and monitoring and reporting on system status.

More resources:
Best Practices & Resources: www.symantec.com/cio
Symantec Enterprise Solutions: http://www.symantec.com/enterprise
Symantec Security Response white papers: http://www.symantec.com/business/security_response/whitepapers.jsp

About Symantec
Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Symantec Corporation
World Headquarters
350 Ellis Street
Mt. View CA 94043
1 (800) 721 3934
www.symantec.com

symantec™ Confidence in a connected world.