TOP 5 TRENDS IN IT SECURITY that every business should be aware of

PlanNet

As many have learned leaving business data vulnerable opens the door to slew of problems with the propensity of technology hacking, hacktivism and internal and external data theft. Implementing solid IT security measures is an essential component of running a successful business in today's complex digital world.

When it comes to the information technology arena, IT security refers to the strategy, processes and tools used to protect the valuable electronic data owned and/or used by your business.

The data which most businesses are concerned with, relates to information considered confidential, and in some business verticals, data which the business is required by regulation to keep safe from unauthorized access. This could be information regarding employees, clients, financials, products, etc.

While most information breaches we hear about tend to be those of large businesses, even a small business can be severely impacted by an information breach or cyber-attack.

"The world of IT security today is complex, expensive and hard to sustain without a suitable security strategy to drive the effort. "

Long gone are the days where a small to medium business (SMB) only needed a good anti-virus tool on their PC's, and a simple firewall to protect them from internet based threats. The world of IT security today is complex, expensive and hard to sustain without a suitable security strategy to drive the effort. And most businesses, large enterprises to small and medium, do not have a viable and sustainable IT security strategy to manage these ongoing threats.

Data loss prevention, internal and external firewalls, advanced security threat prevention, secure firewalls, secure email, endpoint security and encryption are just a few of the common tools that all business types need implanted in their security strategy.

PlanNet

So what are the TOP 5 TRENDS in IT security?

1. **Strategize**
   Execution without strategy is a non-starter. Invest in a suitable and trusted advisor to help develop the security strategy for your business. At an enterprise level, this may be a full-time Chief Security Officer (CSO) or Security Architect. At an SMB level, this means working with a firm that can provide the CSO level advice and ongoing oversight at a time commitment and cost suitable for the size and industry of your business.

2. **Be Proactive**
   

   Protect your business now. Many businesses implement security tools and resources after a security incident has already occurred and impacted their business. In well documented cases at the enterprise level, the ROI by implementing simple tools and processes prior to a security incident would have been over 3,000 times (estimation of license and implementation cost versus initial class action lawsuit against the organization). At the SMB level, incidents are less commonly documented, but ROI's are fairly simple to calculate based on the cost of security versus the cost of a single breach.

3. **Tool Consolidation**
   A solid security strategy today, means that your security toolbox will consist of a number of tools. By selecting a tool vendor that can provide near 'best of breed' tools for each category (endpoint security, DLP, IDS, firewall, secure web, secure email, etc.), this consolidation approach as a strategy will save your business 50-80 percent on the year-1 license costs and ongoing maintenance of these tools over a five year total cost of ownership.

   In an example enterprise customer case, a 'best of breed' cost was $14 million year one, where the consolidation strategy had a cost of $7 million over three years. SMB's saw equivalent percentage savings as well.

4. **Managed Security Services**
   IT security is one of the most complex and costly areas in IT today. Both enterprise and SMB's benefit by working with a managed security service provider, that will help create the strategy, execute it, and manage the ongoing operations of the tools for IT security. A managed security services provider can provide better services for your business, at less cost than the business can provide internally.

PlanNet

5. **Mobile**

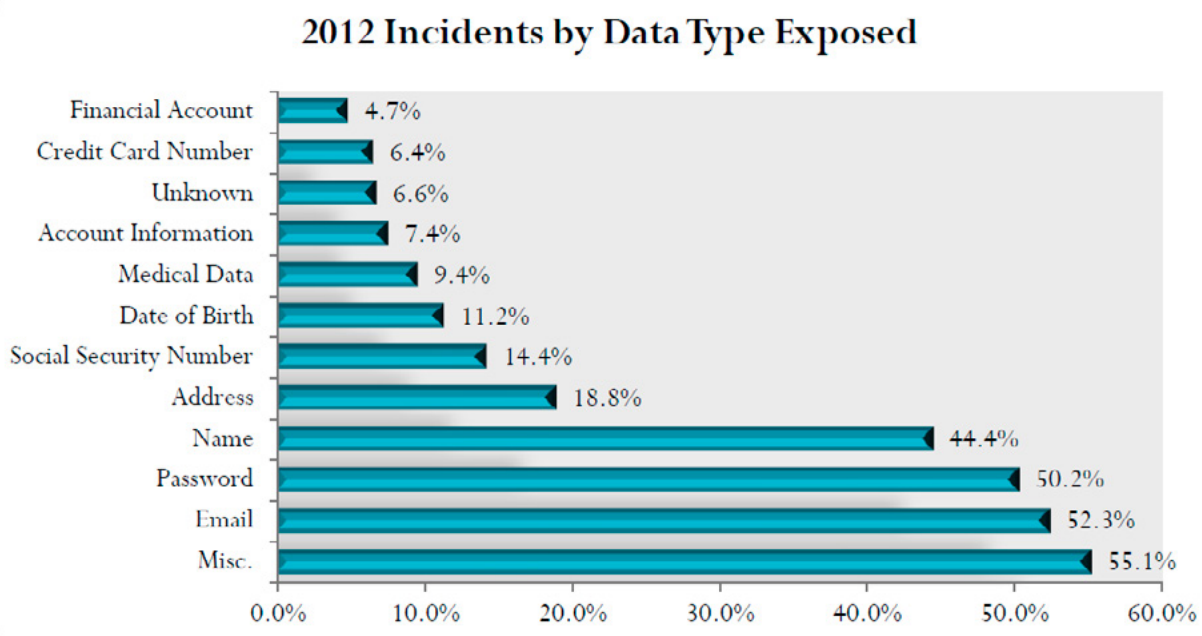
The massive increase in mobile device utilization in business has made the requirement to have a solid IT security strategy even more important. Cell phones, tablets, laptops and cross-function devices are as important to protect as the computer or server inside the building.

In a 2012 security report from Risk Based Security, the number of incidents has more than doubled compared to 2008. The number of incidents in business was 3x the number of incidents in medical and education combined, with over 180,000,000 records exposed.

The primary incident types were:

- email;
- stolen laptop;
- web;
- documents;
- fraud; and
- hacking.

The type of information being accessed and exposed to threats in the following graph, gives both enterprise and small and medium businesses a reality check on what data they own or access, that is a target to those threats that are out to get it.



Source: Data Breach QuickView 2012, Risk Based Security

What next?

Develop your IT security strategy, or get a second opinion on the strategy you already have. Ensure that the advisor with which you are entrusting your business data (and perhaps financial future) is an experienced security specialist with a reference-able track record. Then implement the strategy in a logical and affordable manner that your business can adopt and afford.

PlanNet recently saved a customer over 60% on their overall security strategy. To see if we can help you achieve similar results contact us at info@plannet.com or at 888.557.5266.

PlanNet