

## New security culture needed says IT experts

Caribbean information technology (IT) managers should leverage regulation as the main reason for implementing solid network security policies across their enterprise, advises a senior IT security strategist at McAfee.

Daniel J. Molina, a senior security adviser from McAfee, one of the world's largest internet and enterprise IT security firms, toured the Caribbean in February as part of the worldwide launch of McAfee's new suite of security software products. He says that many business leaders do not really appreciate the importance of network security until its too late and their system has been compromised by an attack and critical data is lost or stolen.

"Much of the investment that is being made into network security has been driven by the need to meet local or international business regulations," says Molina. "For banking and financial institutions in the Caribbean, the international requirements are the new Basel II standards. Additional standards are required for companies doing business in the United States. Fund managers, public companies and traders also need to meet Sabanes-Oxley and other disclosure requirements.

"Although meeting these standards can sometimes be expensive, they create a platform for achieving security best practices and making enterprises more efficient. The idea of security risk management does not just include reacting to threats, but aligning the business processes to they become more efficient and responsive to the needs of users, management and regulators."

He said to deal with the challenge facing businesses, IT, audit and regulation must be closely integrated so that anomalies and threats to the system can be quickly isolated and addressed.

"In reality this is easier said than done, and it is often difficult for IT managers to sell the idea of security to business leaders and network users. When security is required by law or regulators, it is easier to make people comply and develop a better attitude towards corporate security.

"In many enterprises, there is an attitude among some employees that security rules do not apply to them – particularly when they are not on the job, at their desk or if they

are off the network. But if they use a corporate laptop, the company's data still needs to be protected and access must still be restricted and enforced."

While the consequences of an attack can be substantial, the damage to an organization's bottom line from their own security inaction can be even worse. He said from McAfee's research, the main reasons for security breaches are surprisingly simple – and many organizations spend too much time and money on the wrong problems.

A sizable investment is made on reactionary fixes that deal with the immediate issue, but they often fail to address the vulnerabilities, policies and procedures that are at the heart of the problem and the systematic cause of 99 percent of all security incidents.

The problem is that an integrated solution is needed for corporate security. Even when isolated security issues are addressed, for most companies the complexities of running daily operations means they simply do not have the time, or the expertise, to implement a complete security solution. Ever evolving threats, changing business priorities, and limited staff exacerbate these issues.

The next generation of McAfee's security suite seeks to address these gaps in the corporate IT defensive wall. It was developed over the past three years and includes technology from several key acquisitions that can enforce corporate security policy, even when laptops and files are not on the network.

Molina said McAfee's new acquisitions have positioned the company to offer encryption and corporate data protection that can be enforced no matter where the laptop or files are being used.

Corporate policies can be set for a file, a laptop or the enterprise. The security features cannot be overruled, even if you are the administrator of the laptop. It also keeps track of who has access to the computer for auditing purposes.

"Policies can be set to prevent a file from being printed, copied, pasted, moved, emailed or even opened – unless it is on an authorized computer, by someone who has access credentials. These rules will follow the file wherever it goes. This is particularly important for protecting corporate data, financial information, management reports and payroll data.

"For a corporate computer, the user should not be the administrator of the equipment. You are simply a user and corporate attitudes about this must change. Many users put

personal data, entertainment files and internet downloads on their corporate laptop. This is one of the most vulnerable points for the corporate network.

“Many attacks come from within, by corporate users who unknowingly download spyware and malicious software. Because of the security environment we live in, a corporate laptop must only be used for company business and all security protocols must be observed. If these rules are not followed, you will be putting your company at serious risk.”

He said the new suite is complex enough to manage, track and audit complex security issues from a single console to reduce cost of administration and improve return on investment. There is also a low cost small business version of the suite that would be applicable to many Caribbean businesses and IT managers should explore their options for a complete solution that matches their needs and budget.

The newest additions to the suite include four major integrated modules that address specific vulnerabilities. Technology developed by a key McAfee acquisition, Site Advisor, includes a new feature that has mapped the internet and rated sites for spyware and spam. It warns the user about visiting these sites, or they may even be blocked by the administrator.

Another acquisition, Preventsys, helps administrators create and implement a policy that ensure compliance with all regulations and best practices for network and data security. The third addition to the software suite includes Onyigma. This technology protects against data loss. Based on your corporate policy, it can keep track of data and enforces the policy set by the administrator. It prevents cut and paste, attempts to save the file on inappropriate systems, or to email the file to inappropriate recipients.

Citadel, the final addition to the new suite automates the remediation process after threats have been identified and removed.

Although deployment of the new suite is still ongoing in the Caribbean, Dawn Davis Marryshow, a network administrator at Trinidad & Tobago’s Unit Trust Corporation (UTC), said based on reports from testing demos from McAfee, she is looking forward to applying the software on their network.

“The ability to address the issues of audit, compliance and fiscal requirements, together with corporate data policy enforcement makes it very attractive to financial institutions.”

The UTC has to meet compliance issues with local regulators, the Central Bank of

Trinidad and Tobago, as well as US compliance and disclosure requirements as the company operates a US dollar fund.

“Security is always an issue with us because we operate in a very competitive environment and sensitive data like customer account numbers, financial information, background checks and other sensitive data must be protected. This is important not only for the customers but also for us, as it can impact on the confidence our stakeholders have in our operations,” she added.

Trinidad and Tobago Unit Trust corporate has more than TT\$20 billion under management and is one of the largest regionally owned and operated fund managers in the English speaking Caribbean.

“The Caribbean was initially slow in responding to the need to protect sensitive corporate data, but the interest is growing as corporate leaders are seeing media reports on the impact of inadequate security,” says Roan Daley, a senior IT security specialist at InfoTech Caribbean in Kingston, Jamaica.

“Companies are sharing information and data in order to remain competitive and responsive to their customers’ needs, and it is very easy for inappropriate data and information to slip out accidentally or otherwise.

“In addition, in order to improve collaboration and efficiency, more Caribbean enterprises are connected to the internet than ever before, and they are dependent on IT to maintain their competitive edge.

“This means that more Caribbean enterprises are vulnerable to hacking, viruses, denial of service attacks and other risks – just from being connected to the internet. The world has changed and data must be protected from corporate espionage, to safeguard customers’ privacy, to protect your corporate image and to safeguard the corporate network.

“The Caribbean is particularly vulnerable to social engineering attacks, as we still assume that people are always honest in their interactions with frontline staff. Training to prevent staff from releasing sensitive information is still needed, but IT solutions are now available to prevent access to information, as a second line of defense.

Employees will only have access to information they need to perform their duties. Information such as financial data, customers’ accounts, banking information and corporate sales data will remain restricted, thus limiting the impact of social engineering.

“Caribbean business leaders are beginning to recognize these risks and vulnerabilities and they are responding by increasing funding to IT. The boardroom is now awakening to the contribution that IT is making to the bottom line and they are taking steps to protect their networks, improve the functionality of their technology and improve collaboration.

“The new range of integrated solutions as well as the new licensing structure offered by market leaders such as McAfee, will make these security tools well within the reach of small and medium sized businesses across in the Caribbean,” he added.