Resellers provide insight

on security issues, technologies, and management frameworks

VARs are often positioned as extensions of their clients' IT capabilities, able to provide expertise in areas of infrequent need (such as the deployment of a new software package) or on subjects that demand extensive training and focus. Security is perhaps the best example of this latter requirement: public and private-sector organizations are confronted with threats and tools that evolve daily, and with shareholder and regulatory pressure to maintain continuously-effective safeguards against viruses, hacker attacks, data loss, and business disruption caused by malfunctioning networks or devices. For this month's In the Middle, we asked six VARs with deep experience in security to help explain how this technology is evolving within their clients' environments.

1 What is the most common security issue that you encounter within client accounts?

Today's IT departments face numerous security challenges: physical security and client device protection, network threats and data loss prevention, and process challenges ranging from logging and patching to social engineering.

Daniel Reio, CDW Canada: The security issues faced by customers include physical security (lack of a server "room" and the server being accessible by any employee, laptops left in taxis), network security (poorly configured firewalls, denial-of-service attacks), software security (malware, botnets, viruses, spyware) and social and human security (phishing, exploitation of social networks to compromise a user's login credentials).

Brian Bourne, CMS: Every company has different types of assets to protect, and different levels of IT maturity, so commonality is less obvious than a vendor with an agenda may lead you to believe. If I have to choose a single issue, I'll choose malware on the desktop. Malware on the desktop has gone far beyond the traditional virus. Machines join botnets very quietly without setting off antivirus and often going unnoticed on the network. This is a bigger issue than most IT departments will ever admit, or perhaps even be aware of.

Rob VandenBrink, Metafore: We continue to stress logging and log analysis with customers. Surprisingly, as we work with new customers, we find more and more that do not have central logging, and customers who do not count logging in with their compliance responsibilities. Where clients do log, it is historically very common to see that no resources are assigned to review and act on log data.

Stephen Perciballi, Softchoice: 20% of the compromises we deal with are websites compromised by SQL Injection and/or Cross Site Scripting. The remaining 80% of websites are client infections where the user visits a popular, trusted website and gets infected with malware. These client infections are directly related to the compromised websites. If the websites weren't getting compromised there would have to be another way to infect the endpoints.

Aaron Brooks, UNIS LUMIN: Keeping up. It's an interesting time to be in security as the advent of social changes and technology advances such as social media, cloud computing, smartphones, bring your own devices (BYOD) programs, et cetera, are all leaving clients asking "how will this impact me?"

Gary Sohal, Audcomp: Some of the most common security issues are: overall Internet security, to the client and to the network; firewall protection; PCI compliance; internal security (data loss, data protection), security in a virtualized environment (virtual desktops, virtual servers, virtual storage), security in cloud computing, and secure network and-or VPN solutions.

2 What are the most important IT security technologies and processes that you think clients should deploy?

Continued on page 18

IN THE MIDDLE

From left to right: **Daniel Reio,** director of marketing, CDW Canada; **Rob VandenBrink,** solutions specialist, networking and security, Metafore; **Aaron Brooks,** security practice lead, UNIS LUMIN; **Stephen Perciballi,** director of security solutions, Softchoice; **Gary Sohal,** president, Audcomp; **Brian Bourne,** president, CMS Consulting and co-founder of the Security Education Conference in Toronto (SecTor).

Continued from page 15

While responses to this question vary, there is a common theme: Technology matters, but what matters most are frameworks and processes that support a comprehensive approach to security management.

Rob VandenBrink: Security event and incident management – (SEIM) tools attempt to correlate information from disparate components – routers, servers, firewalls, ABM machines – pretty well all networked components within an organization – with the goal of taking seemingly unrelated alerts and making a single incident on a common timeline out of them. While SEIM tools have been available for several years, we are only now seeing them start to realize their potential.

Aaron Brooks: We have to help our clients embrace the changes that are happening in our industry, looking at how deploying BYOD programs, embracing social media and virtualizing your environments can actually help you control information sprawl. Fighting against these advances will be more costly in the long run than planning to adopt them. It is adoption of technology that generates the power of productivity, not the invention or implementation of technology.

Daniel Reio: Some of the most important security technologies clients should be adopting are network security, secure access control and user authentication, as well as email and web security. Ideally, we want to bring the routing, switching, security, and wireless technologies together to enable the corporation to securely access mission-critical services and applications, and pairing this integrated infrastructure with a strong access-control strategy.

Gary Sohal: There are several security technologies that our customers are and should be deploying. These include endpoint security (antivirus) products, network security products (such as firewalls), data encryption, data protection – meaning best practices for backing up – virtual desktops to protect against data loss, and technologies to ensure information confidentiality.

Brian Bourne: Sadly, my response isn't an advanced defence technique. Today, many Canadian IT environments still lack management tools, processes and-or human resources to have a well-managed network. Without the ability to deploy updates and report on what exists in your environment, more advanced security solutions provide limited value. For instance, if you can't tell how many un-patched machines you have, or where they are, and if you have no method to update them or simply hope they self-update from the Internet, then you really have no control over your assets.

Stephen Perciballi: We are focused on four security pillars for 2011.Web security consists of assessing websites repeatedly for application layer vulnerabilities, protecting websites with web application firewalls, and defending endpoints from websites that do not have these protections. Data-loss prevention is going to be phased in slowly and will consist of always-encrypted USB keys, endpoint software for device control, full disk encryption for mobile devices, and network DLP for data in motion. Virtualization security can combine several traditional technologies to secure the new and vast virtual environments: network intrusion prevention, firewalling, and anti-malware, all of which should be in every network today, but have been lacking in virtualized environments.

3 How do some of the emerging IT products and models – like the use of smartphones for mobile access to corporate data, or the use of cloud – impact the threat or security profiles of your customers?

In general, our experts see mobile devices as a source of new and often unmanaged vulnerability. Cloud, too, can expand the threat profile, but it also offers options for mitigating data risks.

Aaron Brooks: This is a topic of hot discussion for our clients, and we firmly believe that adopting these trends will actually increase your security profile… if done right. It's important to realize that these issues are about more than just technology – they impact the business in a number of ways, and proper planning, awareness, education and alignment of business will drive not only a successful program, but also more secure data, which is the ultimate end goal.

Gary Sohal: Our customers fear loss of data and their clients' data. Smartphones and cloud products raise concerns on how to protect this data in this type of environment. Lost or stolen hardware with data on it is also a threat. Overall, data loss is the largest fear – protecting and keeping data confidential. Protecting handheld devices against unwanted viruses or malware is also a high priority – companies do not want endpoints opening up the network to possible virus intrusion so they must find ways for protection of the network, while at the same time allowing the end user freedom to use new technology.

Brian Bourne: As decoupling between platform, application and data evolves, security becomes increasingly complex and specialized. Ideally you want to enable your em-

ployees to be productive regardless of where they may be and regardless of where their needs are most cost-effectively serviced. The challenge, of course, is building and understanding the new threat models that apply to each situation and carefully choosing your investments.

Stephen Perciballi: With data centralized in the private cloud, users want to be able to access it from anywhere on their mobile devices. DLP technologies can help to protect data in the cloud, ensuring that it is encrypted and that the right individuals are accessing it. Mobile management systems allow administrators to bring all mobile device web traffic to the private cloud for interrogation, and ensure that users don't install rogue applications on their devices that could lead to data loss.

Daniel Reio: Data stored locally on smartphones or available through them can become a real security risk. A best practice to minimize risk is to enable password protection on the device and configure it to delete all stored info after a predefined number of failed access attempts. Many mobile devices also offer the option to install apps that can help track and lock the device remotely if lost or stolen. Organizations will have to consider a DLP strategy as they support varying brands of user-owned devices. While cloud computing is in its early stages for most customers, it could offer some security benefits with the centralization of data.

Rob VandenBrink: The key issues with smartphones and tablets are a lack of security mechanisms, and a lack of logging. We are seeing smartphones and especially tablets (iPads in particular) being rolled into corporate processes and tasks with no security mechanisms in place at all – only the functional aspects are being considered. This is disturbing as tablets are often used for sensitive work – as personal stations for executive personnel, for instance.

With public clouds, the major issues are a lack of consideration for compliance, security by signature, lack of logging, and a lack of disclosure on architecture. Public clouds are now being used en masse, but there are several considerations that are routinely minimized or ignored in these deployments: the underlying architecture of the supporting network in the cloud is not disclosed, which opens up customer risks, and a lack of infrastructure logging, security assessments and audits, which are replaced by faith in the signature on the contract.

4 Do your customers view security, privacy, continuity, and compliance as parts of a single process, or as discrete objectives? And from an IT perspective, do you bridge these issues, or deal with them independently?

The best summary of our experts' responses to these questions might be "yes" – yes, our clients view these as discrete issues, and yes, we attempt to manage them within a single comprehensive framework.

Gary Sohal: The larger clients tend to deal with this as a single process. Security is security. We do try and bridge the issues for those who consider security an independent concern – we believe that protection in all aspects of IT will reduce risk.

Brian Bourne: As a function of budgeting, often these are addressed as discreet objectives and efforts. Security protects privacy, but privacy efforts are often a separated from security endeavours. Continuity may be a component of security, but often DR and business continuity are looked at separately from security. Compliance is entirely its own animal. Compliance may drive security, but is yet again addressed by a separate team as a separate endeavour.

Rob VandenBrink: Customers view all of these as discrete objectives, each with a separate budget. We on the other hand attempt to include each of these as requirements within the design of any large IT project. In particular, continuity (disaster recovery, business continuity, pandemic planning and the like) projects all tend to completely ignore privacy legislation, compliance and many other basic security requirements.

Stephen Perciballi: Smaller organizations have better visibility in some respects because it's the same small group of people who manage the entire network. Larger organizations will have storage administration, server administration, application administration, and network operations groups. When these administration groups have their own budgets it is more difficult to help them see between silos.

Aaron Brooks: I found out early in my career that there is no one answer for how people should secure their data: it's about understanding the goals of the business, the risks inherent to how they use information to achieve their goals, and planning accordingly. Part of our role in the process is to help businesses understand IT, and IT clients to understand their businesses.

Daniel Reio: The reality is that security and its relative importance is a matter of organizational focus. Depending on the type of risk being addressed, the facets of security, privacy, continuity and compliance may be individual issues or combined into an overall strategy. For example, an organization going through PCI DSS compliance has a multifaceted task that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. In other situations these issues may be handled independently, like ensuring physical security of a smartphone or laptop or privacy of a company's sensitive data. IT