BEST'S REVIEW
August 2001

Two Worlds Colliding

Illustration by Karen McNamara

The combination of the high-tech security industry's expertise, products and services with the insurance industry's risk-management expertise, products and services could create a new insurance segment.

by Gates Ouimette

Almost everyone involved in information technology is concerned about security, from venture capitalists on the cutting edge to the "laggards" on the technology adoption curve. The insurance industry should be excited by the immense opportunity and companion challenges of capitalizing on this emerging insurance market.

Evidence of a joint vision is being articulated by some of the world's leading technology security experts and insurance thought leaders.The vision is of a venture that combines high-tech security industry offerings with insurance products and services.

Earlier this year, newspapers reported a spate of online turf wars between the United States and China, where hackers from each country played a game of "one-upmanship." What received much less publicity was the news that their hacking predecessors—who are now helping prevent security breaches, rather than doing the "breaching"—are touting the benefits of integrating high-tech security systems with insurance.

Information technology and insurance traditionally have not been mentioned in the same breath—at least not nearly as often as high technology has been associated with the securities industry or the banking industry. But insurers have the unique opportunity to leverage technology as the underpinnings of a new, high-growth, high-profit market segment.While technology is a significant security enabler, the insurance industry knows best how to quantify the risk and create products that address critical business issues. For the high-tech security industry to reach current market projections, it will need the insurance industry in lock-step. According to Datamonitor, an international market research firm, high-tech security product sales are projected to grow from today's $4.5 billion a year to $18.5 billion a year by 2005, with related services totaling another $11.9 billion a year by then.

Techies Tout Insurance

High-tech security experts are trumpeting the benefits of insurance. Not only are these high-tech security leaders bullish about it, they are taking an active role in helping define, lead and implement real business solutions with the assistance of insurers.

One of the world's foremost security experts, Bruce Schneier, has continued to proclaim the importance of a combined technology and insurance approach to security as part of a risk-management strategy. Schneier, founder and chief technology officer of Counterpane Internet Security and author of *Secrets and Lies: Digital Security in a Networked World,* has waved the insurance banner since July 2000, when Counterpane formed a partnership

Gates Ouimette is an independent consultant based in Medfield, Mass., and a member of the board of directors of Pedestal Software, a security software firm based in Norwood, Mass.

with Lloyd's. The venture gives Counterpane clients the option to buy up to $100 million in coverage to protect against the losses caused by high-tech security breaches. "Sooner or later," Schneier wrote in the February 2001 issue of *Information Security Magazine,* "the insurance industry will sell everyone anti-hacking policies."

Schneier's perspective is not unique to the security consulting world. More traditional high-tech organizations, such as IBM and Hewlett-Packard, have long had partnerships with insurance companies, so extending those partnerships into the security space was anticipated.

Other high-tech security consultants and analysts agree about the benefits of integrating IT security and insurance. Philip Cox, a SystemExperts consultant, commented during a presentation in New York in April that the high-tech security industry eventually could come under the auspices of the insurance industry.

Cox, author of the *Windows 2000 Security Handbook,* understands and consults on the importance of increased standardization and the need to decrease high-tech users' security risks. SystemExperts provides a road map to help increase the insurability of any business concerned with risk management. The next logical step for a business, therefore, becomes exploring the risks and rewards of enhancing its existing insurance relationships to encompass its information technology security.

Integration Theories

David Hughes, vice president of Nac Reinsurance, explains the current theories about combining the capabilities of the high-tech security and insurance industries in an article in the February 2001 edition of Professional Liability Underwriting Society's *PLUS Journal.* In the article, Hughes argues that the insurance industry need not change analysis tools; in fact, he states that the industry "must bring historical methods to bear in addressing these new exposures."

"Prudent carriers who are writing e-commerce risks have partnered in some manner with professional security experts who are required to audit the systems security of potential insureds to identify weaknesses and to recommend enhancements," Hughes wrote.

> Information-technology security is a complex issue and can have major consequences to any business if compromised.

Hughes underscores the value that insurers can provide to businesses interested in high-tech, security-based risk management. Just as important, however, is knowing what type of high-tech security products or services can be used for an initial systems security audit and which of these products or services can be used to continually monitor the security of a business's technology.

The good news is that there are several options available to businesses and insurers in obtaining the information necessary to justify purchasing or to write high-tech security insurance. The better news is that these options can be used for monitoring, to identify new issues, to report trends and even to prevent technology's inherent flexibility from becoming too burdensome to securely manage.

From 'Fortress' to 'Airport'

In the earliest days of high-tech security, everything was centralized, and there was mainframe security. As computing became distributed internally through local-area networks and wide-area networks, security products and services needed to function in that environment, although they were still primarily internally focused. With the advent of the Internet, data communication into and out of a corporation suddenly became more commonplace. Security products and services for the "Internet age" were first built in what is commonly called the "fortress" model: Firewalls were installed to keep out unauthorized users. As these "invaders" became more sophisticated, the firewalls became more complex, but they were still being sold, and used to create a fortress.

With the advent of intranets, extranets and online business-to-business exchanges, the "successful" high-tech security model evolved to support business functions. Rather than being a fortress, high-tech security now uses more of an "airport model," according to Jonathan Gossels, founder and president of SystemExperts Corp.

Gossels uses the analogy of an airport security system to describe the evolution of high-tech security products. Credentials for information-technology users—internal and external—should be coordinated through an authentication process, a systematic approach to assigning rights and privileges based upon who the users are, what IT services they need to use and what business processes they are involved with. Like an airport, these high-traffic high-tech systems are much more than just user-based (e.g., passengers). Rather, the high-tech security system also supports employees (e.g., who is allowed on the airport tarmac), partners (e.g., food services) and vendors, and it has different security levels based upon different, dynamic events (e.g., politician arrivals).

The complexity of using the "airport model" for security should be apparent. The evolution of high-tech products has been reflected in the increased sophistication of high-tech security products and services. Initially, the security products had been point offerings, addressing a niche (e.g., firewalls). As the industry has matured, the more established information-technology security vendors—such as Checkpoint—have begun espousing the benefits of an overarching architecture. Checkpoint's OPSEC (Open Platform for Security), the recent winner of an industry award for the "best enterprise security framework," is a fairly comprehensive grouping of partners, certification, a software-development kit and the framework itself.

Underneath any security framework, different security layers are typically defined as host security, firewall security, connection security, encryption and digital certificates and signatures. Since the actual architecture implementations are still emerging, when evaluating high-tech security solutions, it is important to consider product and services vendors offering multiple solutions across multiple platforms that can "grow into an architecture." A sample reference chart of these vendors can be found at *www.checkpoint.com/opsec/allopsec.html.*

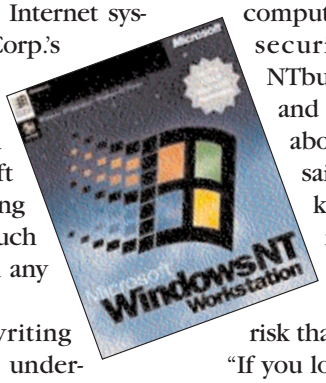
A critical area that someone analyzing security requirements should explore and understand is the role of Lightweight Directory Access Protocol (LDAP), which is typically the main "entry point" for user access into an information-technology environment. As the security frameworks mentioned earlier become more prevalent, the role of LDAP and its importance to information technology security will continue to grow exponentially. A key example of this is that although LDAP servers themselves conceptually fit into the host security layer, their impact spans multiple security layers. As digital certificates are increasingly stored in LDAP servers, something compromising the security of an LDAP server would affect a company's digital certificates. The result would be a compromise of a company's three basic security functions:

- authentication: who the user is;
- authorization: what the user is allowed to do; and
- accounting/administration: user reporting.

Information-technology security is a complex issue and can have major consequences to any business if compromised. Combining the high-tech security industry's expertise, products and services with the insurance industry's risk-management expertise, products and services holds significant promise. The power of the Internet and its impact on business has only begun; to remove inhibiting concerns via a solid risk-management approach would be of significant value, indeed. BR

E-Business Insurer Raises Premium on Windows NT

An insurer specializing in e-business risk underwriting said it will charge 5% to 15% more to cover the risk of hacker attacks on Internet systems that use Microsoft Corp.'s Windows NT software, claiming it has identified certain claims trends in those systems. Microsoft disputes the finding, saying its hasn't heard of any such trend in discussions with any insurance carrier.



J.S. Wurzler Underwriting Managers Inc., a Lloyd's underwriter, said claims experience shows that NT-based systems tend to suffer more downtime as a result of hacker attacks than other operating systems. John Wurzler, founder and chief executive officer, was quoted in *Interactive Week* as saying, "we saw that our NT-based clients were having more downtime" from hacker attacks.

Microsoft spokesman Jim Desler said he didn't have any information on Wurzler's action and that Microsoft hadn't heard of any such concern from other insurers. "None of the carriers we deal with had said any such thing," Desler said. "Internet and Web site security insurance is a new business. We believe there is not enough information about the business to judge such risks accurately."

Russ Cooper—a computer security expert with TruSecure Corp., a computer risk-management and security firm, and editor of NTbugtraq.com, which tracks and disseminates information about Windows NT systems, said there is no method he knows of that would make sense in singling out Windows NT software as a greater claims risk than other systems.

"If you look at reported instances of security problems, Unix-based systems are 10 times riskier than NT," Cooper said.

Robert Hartwig, chief economist with the Insurance Information Institute, said insurers that specialize in Internet and e-commerce underwriting have just begun to gather enough claims experience to fine-tune their pricing. "What you're probably seeing here is the discovery of a new rating system," Hartwig said.

He compared Wurzler's move to what auto insurers did in response to sport-utility vehicles.

"There are certain factors that influence pricing in a particular line," he said. "Apparently he identified Windows NT as one of those factors."

S.C. Blues Offers Online Claims Filing

Blue Cross & Blue Shield of South Carolina said physicians can file health-care claims directly via its Internet sites, saving time in payment turnaround and minimizing filing errors.

Physicians who have gone to SouthCarolinaBlues.com, CompanionHealthcare.com or HMOBlueSC.com to register a profile in the secure section, called "My Insurance Manager," can fill out information on these claims and submit them there. The claims are sent directly to the company's data-processing center.

The system does an immediate check for errors and informs the physicians if there is information missing or incorrect, according to Blue Cross. Physicians can check online the next day to see if the claim has been processed, saving time traditionally spent on the phone.

Besides submitting claims online, physicians also may submit referrals, check the status of a patient's claim, check eligibility, view benefit booklets, check authorizations and referral status, see how much patients have paid toward their deductibles and out-of-pocket amounts and confirm whether a patient has any other health insurance. They also can submit a question or comment online with secure messaging.