Ensuring Business Continuity Through Security and Privacy

EDITORS' NOTE *The number of ways corporate security can be breached, and the privacy of companies invaded, seems to multiply at a disturbing pace year by year, leading enterprises of all sizes to take a fresh look at their risk exposure.*

As the disciplining effects of Sarbanes-Oxley begin to be felt, turning a spotlight on the internal workings of corporations, LEADERS Magazine assembled a group of executives and professionals to share their thoughts on how companies can – and should – protect their valued assets.

In the pages that follow, the industry leaders listed, right, discuss operational risk management and the symbiotic relationship between three critical challenges of the post-9/11 world: security, privacy, and business continuity.

Decker: Some of us here have known each other for many years. For example, Alan [Brill] and I have known each other for 25 years, ever since I started in the security industry, when password protection was pretty much the extent of it. Today, in my view, we have enough technology to secure the entire world. The problem is, in many cases, the most important technologies are under-funded or improperly applied, implemented, or maintained; or worse yet, there's a lack of overall interest in them. In light of the serious attacks on national and international security, it's hard to understand why some organizations aren't hopping on the security-and-technology bandwagon as quickly as possible.

Aucella

Brill

That said, I believe many organizations have well-defined security programs, particularly in the financial-services sector, which has always been on the leading edge of technological security. In addition, more manufacturers, retailers, and health care companies are now taking a closer interest in security, privacy, and business continuity. They are realizing that one slam to their security system can shut down their production lines or point-of-sales systems for an entire business day, completely disrupting their supply chains. This reality is now starting to sink in, due to certain current events. The attacks of September 11, 2001, were physical, and raised a strong reaction from many CEOs and boards of directors. Rebecca [Whitener] and I have been in more rooms in the past year and a half than we have in the past 15 years because of the increased interest in security and privacy. After 9/11, the threat of privacy violations became more of a concern at the executive level of organizations. Our clients now want everyone clearly identified, so we have seen an increase in requests from client organizations for identity-management tools to be used on their employees, suppliers, and customers.

The recent corporate-governance debacles and the subsequent regulations initiatives have also generated interest in reducing risk and increasing security and privacy through technology. Our clients are beginning to realize that security- and privacy-related technology is truly a facilitator of business continuity. In today's tricky environment, companies are struggling with three major challenges – security, privacy, and business continuity – as well as corporate-governance regulations and, in some cases, the rebuilding of consumer trust. For instance, last year, a backroom processing company for credit-card companies was broken into. One credit-card company executive said, "One more hit like this and people will stop using

PARTICIPANTS

Joseph Aucella
Director of Information Technology, Ethan Allen Interiors, Inc., Danbury, Connecticut

Alan E. Brill
CISSP, CFE, Senior Managing Director, Technology Services, Kroll Inc., New York

John C. Carrow
Vice President and Chief Information Officer, Unisys Corporation, Blue Bell, Pennsylvania

Albert H. Decker
Executive Director, Security and Privacy Services, EDS, Plano, Texas

Garrett Dietz
Managing Director and Chief Administrative Officer, Towers Perrin, Stamford, Connecticut

Mark W. Doll
Director, Americas, Digital Security Services, Ernst & Young LLP, New York

Herbert M. Greenberg
President and Chief Executive Officer, Caliper Corporation, Princeton, New Jersey

Stanley Quintana
Director, Security Services, AT&T Corporation, Bedminster, New Jersey

Patrick Sweeney
Senior Vice President, Corporate Communications, Caliper Corporation, Princeton, New Jersey

Rebecca Whitener
Director of Privacy Services, EDS, Plano, Texas

Carrow

Decker

their credit cards on the Internet." Just think of the business impact that would have. So it's obvious how much security and privacy issues can affect a business's bottom line.

Whitener: I agree. Ever since the tragic events of September 11, 2001, companies and individuals alike have come to realize the key interplay between security – both physical and IT –, privacy, and business continuity. In the past there may have been some degree of separation between those areas of responsibility within organizations. Today, total enterprise security comprises components of both physical and logical security, privacy, fraud prevention and investigations, and effective controls to counter both external and internal threats. Industry analysts suggest that security and privacy and the legal issues surrounding digital signatures represent significant barriers to the future of e-commerce. But are organizations making the necessary commitments to security and privacy measures? For those of you who act as consultants, have your clients initiated discussion on security and privacy issues? Should we be concerned – as citizens and as members of the security, privacy, and technology professions – that there's not enough emphasis being placed on securing corporate assets by individual organizations?

Doll: This is a major issue, and it's appearing in the press more and more these days. In light of Sarbanes-Oxley, there should be a dramatic change in corporate management as these issues come together. On the security front, I haven't seen a particularly dramatic change in the way companies are managed. One reason may be that it's hard for a C-level executive to justify a large investment in security when earnings are down. Very few executives have adopted a proactive attitude toward security and safety. Of course, there are some who want to play defense and be safe, and will publicly and privately communicate their emphasis on security, but they are few and far between.

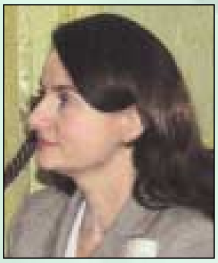
Dietz

Doll

Greenberg

Quintana

Sweeney


Whitener

So, while there is an increase in concern over the technical functions that need to be in place to guarantee effective security, there is a big gap between that heightened concern and the implementation of the security functions that today's commercial climate calls for. In my view, security professionals need to speak to executives, in terms that they can understand, about the risks they run if they don't implement certain security measures. Then it takes true managerial determination to bridge the gap between concern and implementation. Ten to 20 percent of our clients have made the connection, and are implementing necessary and significant changes. Of course, there's also a difference of opinion among security professionals about what processes actually improve security, and that leads to further delays.

> **"*It's hard to understand why some organizations aren't hopping on the security-and-technology bandwagon as quickly as possible.*"**
>
> *– Decker*

Decker: Imagine that: an argument among security professionals!

Doll: Right! Six security professionals will give you eight different opinions. The industry lacks the consistent vision and leadership it needs to move forward. We're experiencing a threefold witching hour: Privacy legislation such as, GLB [Gramm-Leach-Bliley Act] and HIPAA [Health Information Portability and Accountability Act] creates pressure on one side, Homeland Security is pushing from another, and on the third side, Sarbanes-Oxley demands that executives sign off on their internal control systems or potentially face criminal charges. These three factors are giving rise to a major change in thought processes around security. People are just now starting to ask: "What are my responsibilities? How will this work?" That's why there have been some delays in compliance with these rules and regulations; it's hard for organizations to wrap their minds around these issues within the time frames the regulators originally set. This is a difficult transition period, and it may take a while to get through it.

Quintana: I think so many corporations are proceeding cautiously in implementing security measures because they are trying to identify their biggest risks first and then identify the applicable solutions to alleviate those risks. AT&T has found that a lot of corporations have stepped back and asked: "How do we qualify our risks, and how do we mitigate them? What do we really need to put in place? How do we approach this properly? How can we measure the solutions we put in place?" Boards of directors are looking for a methodology with which they can approach risk mitigation. Every time we go into a boardroom, we hear variations on the same theme: "We have a certain amount of investment dollars available for reducing security risks. What should we go after? How can we ensure that our investment dollars are applied to the highest-risk areas in our corporation?" We get a lot more action when we show board members how to solidify and quantify their risks, and then show them the right programs for addressing those risks. The corporations that don't take that approach are the ones that are most likely to misspend their IT dollars.

Doll: How successful have you been in selling that risk analysis to boards? I ask this because many of us use the same approach, speaking to boards about return on investment [ROI], risk management, risk-adjusted returns, and many other components. And many times there's debate over what the risk formulas should be. There doesn't appear to be a standard for those things.

Whitener: It's difficult to set standards because each client organization has a different strategy for the future. Often, companies don't have a well-developed plan for security-risk acceptance or tolerance. I agree that boards prefer to speak in terms of enterprise risk management rather than security. Security is complex and has traditionally been discussed at a technical level that has caused the board to glaze over. On the other hand, boards are used to dealing with business risk issues. When security can be articulated from this point of reference, it is less likely to be passed off as just an IT issue. There needs to be a comprehensive way of addressing security issues as part of the overall enterprise business risk-management process. Unfortunately, it's difficult to communicate with a board about the business risk issues around security when there is not a clearly defined organizational risk-management approach.

Quintana: We use a best-practices approach in addressing business continuity and security, because it demonstrates to corporate leaders that risk management is truly a governance structure. Through that governance structure, the leadership has full knowledge of the risks, can delineate the risks, and can put the necessary programs in place. If you can't get through to executive-level clients, risk-management strategies are just dead, academic ideas. In one sense, risk is just a tool to show a board or executive the value of an investment on a business level. There is no standard in the industry.

> **"*Six security professionals will give you eight different opinions. The industry lacks the consistent vision and leadership it needs to move forward.*"**
>
> *– Doll*

However, at AT&T we've adopted a very comprehensive program that we use with our customers called the Light Bulb All Risk formula, which was adapted from the governmental Trident Approach. The formula takes a comprehensive look at risk beyond just a financial perspective; it examines IT and other components, and very simply quantifies certain risks so that our client organizations' executive management teams can figure out what investments should be made against those risks.

Brill: President Eisenhower once said, "Things are more like they are now than they ever were before," and I really understand what he meant. One of my colleagues recently relayed his experiences from a meeting he had with the senior officials of an insurance company. He said they clearly understood the risks they were facing, but that they didn't feel the pain. And if they don't feel the pain, why should they spend the money to address those risks today? Why not just spend it tomorrow? That's very scary. Kroll is a firm that gets a call right after something horrible has happened. Then we have to investigate what happened: who was involved, how the crisis occurred, and how the organization can resolve the problem. It's very hard for these companies to take a longer-term look at a problem and act before disaster strikes.

For instance, following the Microsoft litigation, people started realizing that they don't want to save every e-mail in the history of the company. So they installed programs that automatically kill e-mails after a certain period. However, Sarbanes-Oxley says there are a number of circumstances under which you should save your e-mails. It took a long time for people to understand that the term "security" referred to technological as well as physical security. Now people have to understand that security also encompasses legal components, such as the interpretation of Sarbanes-Oxley, HIPAA, or relevant court decisions. So computer evidence is now a third leg on the security stool. Traditionally, IT people had a limited interest in spending time with legal counsel. Sure, lawyers would look at IT contracts, but they weren't IT advisers. Now they're strategic advisers to IT departments.

Companies need to recognize this integration and realize that not every disaster is on a par with 9/11. There are smaller disasters that companies don't often plan for. In our work in data recovery, we continually hear from companies going through small crises. Somebody's laptop lost the most important data in the history of the company. Up until this point, companies would just look through a computer magazine and hope to see an ad from a company that could solve their IT security problems. You simply can't run your business that way any longer. Security professionals need to establish the same clout as financial professionals, because our services receive the same amount of attention and planning in their implementation. And by the same token, CIOs need to be far more associated with C-level activity.

Decker: Alan, I think you hit a key point when you mentioned that companies are reluctant to spend on security when they don't feel the pain. Many organizations won't bring in security professionals until after the horses have fled the barn. That's because, in many cases, it's very hard to project what might happen. When my kids were little, we would idly drive through the countryside on empty roads, and I would blow the horn every once in awhile. My kids would ask, "Dad, why are you blowing the horn?" To which I would respond: "To keep the elephants away. You don't see any elephants, do you?"

That story applies to our current predicament. We have to sell our services based on invisible future events. After the World Trade Center disaster, the worldwide network of one of our clients was down for six days because of the Nimda virus. When they asked us, "Why did we get hit so badly?" we had to tell them they had been hit because they hadn't invested in antivirus software. They had decided they couldn't justify the costs because they had never had a virus problem before. The estimated cost to repair their system was 1,000 times what it would have cost to install the antivirus programs. Now they have those programs, but it's after the fact.

Brill: That attitude is a significant problem. In selling that kind of software, you can't point to the ROI because the math just won't scale. That software should be installed simply because a company should have it. There's no law that says you should lower your cholesterol if you have a high cholesterol count. Yet, it's a good idea to take care of it. That ideology applies to the issues we are dealing with. We can use as many calculators and pads of paper as our clients care to see, but it's virtually impossible to come up with any rational mathematics that indicate a company should take certain technological security measures. Nevertheless, sometimes they just have to take them because the risks are too great otherwise.

Quintana: If you have a good risk-management program, it'll tie ROI to a risk at hand. That's why it's necessary to have a comprehensive risk-management program. If you approach a boardroom without a plan for ROI, you might as well not go in. Regarding Mr. Decker's point about unrealized risk, corporations have had the ability to put solutions in place to mitigate risk for some time, but they haven't acted upon those solutions because those risks weren't recognized. Legislation such as Sarbanes-Oxley and HIPAA have been helpful to our cause because they acknowledge that potential risks exist. I think corporations are being minimalist in addressing these regulations because they don't feel the pain. Enforcement at a consumer level and not a government level, will cause the pain. In my view, Americans are litigation happy. So when consumers start filing suits over violations of the new legislation, companies will begin to address the requirements laid down in that new legislation.

> **"*Companies would just look through a computer magazine and hope to see an ad from a company that could solve their IT security problems. You simply can't run your business that way any longer.*"**
>
> *– Brill*

Decker: Rebecca, you often say that, when a company's internal systems are attacked, consumers recognize that the company is the victim of a hack. However, once that attack impacts their personal data or inconveniences them, the company becomes a villain, rather than a victim, in the eyes of the consumer. With that in mind, I think it's necessary to change the overall corporate culture surrounding security. I think all security professionals will agree that an accepting corporate culture is integral to the success of any security program. According to statistics from the META Group, security technology accounts for 20 percent of the implementation of risk solutions, while people and processes are responsible for the other 80 percent. So culture is a key issue here. Security technology and processes have to be embraced within an organization in order for them to be effective, and, additionally, consumers need to be better educated about these matters.

> **"*What is the ultimate responsibility of a private provider, a baseline product provider, or a software provider?*"**
>
> *– Quintana*

Brill: How long have we talked about the technology industry's need to build security and act in a way that makes sense? Kroll is now dealing with a company that was hit, and the account that was compromised was one that the company provided to a vendor with relatively little security. Our client explained that they had tried to strengthen security, but the vendor went nuts and said it would be inconvenient. As long as companies let vendors or other constituencies get away with that attitude, security will be compromised. So we have to address security from several angles; we have to be able to insist that, should our clients' vendors supply software, that software must provide a basis for trust. In the end, true security requires action by our customers, all of their customers, and by all of their user groups.

Quintana: That raises an interesting question. What is the ultimate responsibility of a private provider, a baseline product provider, or a software provider? One of the largest software providers in the world provides some of the most open software in the entire world. If that's the case, hardware and software providers have to accept the responsibility for those products.

Doll: If seven big financial institutions decided they wanted more secure software, you'd have more secure software in a second. Everybody has a different determination of the risk model, and that discrepancy is caused by heroism. New York financial institutions, in particular, have confidence because of the way they were able to recover so quickly after 9/11. But that happened because ordinary people did extraordinary things. People worked 24 hours a day for days at a time to get systems back up. Everyone did the right thing within their organizations, and there were none of the normal internal political battles to hold things up. Everybody just rowed in the same direction. People were fighting for their companies and for America. That process was wonderful, but it's given companies a false sense of confidence in their ability to recover from security catastrophes. People may have an inflated vision of the resiliency of their organizations, and they may be relying too heavily on heroism to fix the next big problem that arises.

Decker: That's right. And of course, time has healed some of those wounds, and people are apt to forget just how terrible that time was.

Quintana: I think that heroism accounted for about 20 percent of that recovery, and fundamental due diligence accounted for another portion. For example, AT&T built and implemented what we call "inter-survivable" networks running under the World Trade Center towers. Those networks were able to survive the events of 9/11, withstand the move of nearly 8,000 traders to New Jersey, and resume activity within a reasonable time frame. So, from a business-continuity perspective, a lot of due diligence was done. But of course, there was a gap that heroism helped to close.

Carrow: We're far better at reacting than acting because this is an abstract area. Security measures are seen as unproductive from an earnings-per-share perspective. So the issue is quantification. I'm curious to know how you all quantify your performances. Can you answer a board when members ask, "Are we secure now that we've spent all of this money?" You'd be a fool to answer that question because it's not answerable. That's the hardest part of implementing security processes, whether for business continuity, disaster recovery, privacy, or in reaction to HIPAA. How do we measure what's good enough? I don't think there is a universal measure of that.

Dietz: I think boards see most issues, including security, as elephants waiting to stampede the boardroom. However, the lack of emphasis on security has been exacerbated by the state of the economy over the last few years. It's difficult to make a case for significant, incremental investment in security when the risks, in many cases, are not truly perceived and significant consequences are not always evident. No one remembers the success of the investments made in Y2K solutions even though a lot of money was spent and things went smoothly.

Carrow: But nobody noticed!

Dietz: Right. And nobody noticed because we were so successful in getting ahead of these problems. Our principal task – and fundamental challenge – is to communicate in practical terms, to boards and senior management teams, the value of investments in security. If we don't navigate leaders through the conundrums, investments won't be made properly. Firms will end up with too little security or too much – and both situations are potentially problematic.

Furthermore, we also face issues of confidentiality and integrity. And we have to provide security parameters without dramatically impacting the availability of information. Our clients have thousands of people worldwide who want and need to access information. So we have to establish the disciplined behavior necessary for protection without negatively impacting this access and the associated productivity. Those are our key challenges.

Carrow: I agree. And I keep looking for a symbolic thermometer, if you will, that will help us communicate security risks, or a lack thereof, to our clients.

Whitener: Clients often say: "Give me the score. I want to know where I stand in comparison with my competition." Many times, companies want to be as secure as competition, but not more so. They don't want to spend any more than their competition unless they feel they can use it for competitive advantage. But at the end of the day, most companies just want the risk to go away. So we have to explain the confidence and peace of mind that can be achieved through investing in effective security.

> **"*Can you answer a board when members ask, "Are we secure now that we've spent all of this money?" You'd be a fool to answer that question because it's not answerable.*"**
>
> *– Carrow*

Quintana: We can never mitigate 100 percent of a company's risk. But we can demonstrate to the management what 85 percent risk mitigation will mean to the company. Security is a hard sell and a unique animal because it's a practice and not a product, per se. Even the most robust solution will have a few holes.

Doll: Absolutely. In our work, we provide attack and penetration services to our clients in order to define their security levels. This year, we had hacked into the systems of 192 companies by July. So if someone wants to get access to an organization's records, more than likely, he will be able to. Even if you spend $20 million on it, no system is foolproof.

Carrow: It's very interesting to walk through a disaster-recovery program for a large corporation. Each business unit identifies its particular problem as mission critical. So you have to prioritize the problems by assessing their recovery times against their impact on the bottom line. That's a fairly rigorous process, if done thoroughly.

Quintana: Then, after you triage those tasks from a business-impact standpoint, you have to evaluate which processes are most at risk to exposure.

Carrow: Yes, we have to identify the threats.

> **“People in my position want to have clear choices. I want an IT expert to keep me informed and install the systems to solve our problems.”**
>
> *– Greenberg*

Quintana: And the associated vulnerabilities. We treat risk management as a comprehensive program because that's what executives want to see.

Greenberg: I have one claim to fame in this group: I am, without a doubt, the least knowledgeable in this arena. But as that and as a consumer of IT, I can contribute a couple of things. People in my position want to have clear choices. I want an IT expert to keep me informed and install the systems to solve our problems. Caliper is now dealing with much larger companies than ever before, and these larger companies have larger IT demands. So I expect technology professionals to educate me on security risks. How much do I need? How important is it? As a consumer, I am frustrated when I hear, “Our system won't let me perform the function I want it to.” We spent a few million dollars on this system and it's supposed to be our workhorse. But sometimes it feels like it's adding to our workload, not making life easier. As a consumer and as a person who has been dragged – kicking and screaming – into the information age, I know technology is an integral part of conducting business today. So technology companies should be in a position to explain to me the benefits of their products and services. It might not occur to me to ask the big questions, so I need someone to explain the reasons why I should invest a certain amount of money in technology, rather than in a marketing program that might bring me noticeable sales increases. In short, I need direction in order to understand how technology can solve my problems.

Aucella: That's a good point. Technology has to be evaluated upon the core competencies it will bring to the organization. I often use an arrow as an analogy. The shaft of an arrow is the wisdom, ideas, and collaboration of a company's people, and technology is the tip of the arrow. Technology allows a company to pierce certain opportunities and move on them.

Quintana: If technology can act as a transformation agent and as an impetus for change, then every company should use it to solve immediate problems and pave a smoother road for the future.

Decker: Herbert, I think that your perspective as a consumer is extremely important. It's of great benefit to us to hear your issues as a consumer of technology in the realms of security, privacy, and business continuity. It's our job to interpret your concerns and develop solutions to support your business.

Dietz: Let me jump in with another example of the necessary balance needed for security. Storage requirements are growing astronomically, and companies are now placing storage limits on their employees. As a result, employees are cleaning out their e-mail in boxes and their extraneous files. Companies think this is a great idea because they'll end up saving millions annually in storage space. However, it's natural for people to save those supposedly deleted files to a CD or Zip disk, or store them on their personal computers. This results in a lot of formerly secure data being thrown into a very vulnerable environment. So, in saving money on the storage end, we can unwittingly cause a major security weakness in our systems.

In my view, security professionals should be engaged in business decisions of this nature, because of the unintended consequences that can result. We need to illustrate how natural human behavior can exacerbate security risks. In other words, we need to show how behavior and security cross paths, and then highlight the ways to mitigate risks associated with that interaction.

Brill: In this high-tech environment, it's easy to forget that security is high-tech, low-tech, and no-tech. I visited a client recently and asked a gentleman who was sitting at a desk working on spreadsheets where the men's room was. He said, “I have no idea; I'm a temp.” Theoretically, this man was working on security-sensitive information. Organizations that wouldn't let an employee anywhere near a computer without a comprehensive background check, and a signed, bonded nondisclosure and confidentiality agreement are afflicted with myopia: They welcome vendors, temps, and so on into their organizations. So security is a weak-link concept from the beginning. A company can install all the latest technological bells and whistles money can buy, but without low-tech security, that technology sits on a weak foundation.

Dietz: That's right. Significant risks exist just because of basic human behavior. That's why we have to link both the technology and people issues.

Carrow: You hit a key point in bringing up discipline. Sarbanes-Oxley and other regulatory controls are forcing companies into developing more coherent forms of corporate discipline. However, the idea of introducing increased and uniform discipline raises some issues. For instance, in an entrepreneurial company, executives want their people to innovate and stretch boundaries. So, as regulations drive corporations toward greater discipline, could the vital spark of creativity get snuffed out? In my view, too much discipline slows down processes and stymies creativity.

Whitener: Companies often see the advantages in collaboration with third parties, business partners, vendors, suppliers, even competitors to increase efficiency, reduce costs, and improve revenues. But companies may be reluctant to pursue those opportunities if they are not sure of the effectiveness of their security controls. As security professionals, we haven't done a sufficient job in spreading the message about security being a business enabler. We haven't said: “Move forward in good faith, Mr. CEO. Collaborate with third parties as you see fit in order to increase your revenues, reduce your costs, and make your organization more efficient. Our security will allow you to do it.” Security needs to be built in, so that our clients don't have to worry about security as they conduct business.

> **“Technology allows a company to pierce certain opportunities and move on them.”**
>
> *– Aucella*

Years ago, after the Treadway Commission hearings, an internal control framework referred to as COSO was established by a committee of sponsoring organizations that included internal auditors, controllers, IT auditors, public accountants, and other professionals. It was, and is, an effective structure for organizational financial, accounting, technology, and management controls, but, as a set of voluntary guidelines, it had no teeth. Sarbanes-Oxley has added the teeth – up to and including jail sentences. Now there is some accountability at the board, CEO, and CFO levels for the effectiveness of internal controls, which can certainly be construed to include security of the information technology systems and processes.

Brill: Any time it's possible for management to do the "perp walk," people take legislation and regulations seriously. That makes it more difficult for management to take the easier, or cheaper, road.

Whitener: Exactly. Sarbanes-Oxley places the accountability for controls at the senior management level, where they can not avoid responsibility by saying, "I didn't know." If you consider security as similar to the brakes on a car, IT controls and security become a mechanism that should be taken for granted as essential to keep an organization running effectively.

> “**_Business continuity relies on the right people having the ability to access the right information at the right time._**
>
> *– Doll* ”

Decker: Yes, precisely. Brakes exist because it makes sense to have a mechanism on a car that stops it from moving. You wouldn't get into a car that couldn't stop.

Greenberg: And brakes allow you to go faster because you have confidence that you will be able to stop.

Quintana: I don't want to sound like a commercial, but AT&T considers its network to be part of the critical infrastructure of the United States. When we began to focus on business continuity, security practices were not in vogue, but they were critical to our customers, the government, and the economy. Fifteen years ago we knew that we had to put business-continuity programs in place that would ensure our ability to recover our critical infrastructure rapidly, on a real-time basis and on a longer-term basis. We did the same thing with security measures. Those initiatives made business sense because we were supporting our customers. Of course, our main priority is to make sure our networks are up and running, but business-continuity practices and security practices are associated with that ability. I believe common sense can be as important as regulations.

Carrow: A constant dial tone is the fundamental requirement of your business. The security industry is maturing to the point where people recognize every business has a fundamental like your dial tone. Physical security used to be the norm because the threat model was a physical break-in to an installation. As functions have become automated and the Web has become the primary means of communication, people have noticed that the threat is broader than someone physically breaking in.

Greenberg: Would you want to do business with a bank that didn't lock its vaults? I believe the concept of security, even in the most abstract sense, can be expressed as simply as that. When someone throws a lot of technological jargon at me, I want to say, "Don't talk to me about IT. Talk to me about solutions."

Quintana: It's important to bring those things together and see technology as a vehicle for business transformation. So, clearly, it's important to have people in place within your organization who are equal parts technology experts and business-transformation experts.

Doll: Business-continuity professionals are generally able to bridge the knowledge gap better than security professionals. In large companies the business-continuity people often influence IT decisions, and those are the people who continue to get promotions.

Whitener: Looking to the future of corporate organizations, security needs to be embedded in the processes, technology, applications – the entire business architecture. We're seeing signs that security is moving in that direction – toward a more intelligent process, where human interaction, monitoring, and decisions can be replaced by adaptive software and hardware. So the requirement for a person to evaluate vulnerabilities or risks will be removed because that evaluation will already be built into the applications or systems. Is that level of automation valid, or even possible? What do you think?

Carrow: In terms of privacy and security, I think business processes will become systemized. But I'm not sure that everyone has accepted the cost consequences of that. Such automation might initially take some speed out of the system as well. Thus, if automated technological features are implemented, it's imperative that the systems are speedy, so that companies can continue to move with agility. Otherwise, they'll lose their competitive edge.

Doll: Business leaders often say that it's all about access. Business continuity relies on the right people having the ability to access the right information at the right time. As such, you can't simply shut down an organization's networks in order to install security features. Ernst & Young has seen more companies invest in securing the lower parts of their networks, routers, and operating systems rather than new applications. Application software is buggy. Anyone who has run large application-development groups over the last 20 years will tell you that during the rollout of systems, you have to tighten security. So, to tie in the brake analogy, you move the car slowly and tighten the brakes before it starts moving too quickly.

Quintana: I think a few thoughts need to be connected. Rebecca's question recalls the early days of embedded financial controls and embedded systems applications. We still need an external human interface to make sure those controls aren't being modified, and the same is true in the realm of security. In nominal approaches technological intelligence can detect problems at the network level without human involvement, but we can't forget the end game: the protection and security of our information.

> “**_IT controls and security become a mechanism that should be taken for granted as essential to keep an organization running effectively._**
>
> *– Whitener* ”

For example, we recently introduced for our foreign Web-hosting customers a product that provides security for Web transactions in the content mode. Now, no one can spoof a transaction, but that's not sufficient. We still have to have people protecting our customers' information. I talk to big financial firms three or four times a week, and they're very interested in applied application control – in people controlling the information through applications.

Brill: Everything we've discussed comes back to one point: Security needs to become something we don't have to apologize for. Security is a presence in an organization because it has to be there. If a company has an accounting system, the company has the right to expect that the numbers get crunched correctly because that's what accounting systems do. So, in that same sense, top management has the right to expect that, if they invest in a security system, they won't have to think about how the technology works. All of the functions are just under the hood, so to speak. All they have to do is turn the key, if you will, and they should be able to drive. In other words, the system should work. That's all that executives need to know.

Greenberg: That's right. Executives don't need to know how the gas ignites in the engine. ●