

Are You a Technical Guru or an Enlightened Friend?

In order to get the information security budget you need, you must be able to communicate comfortably with non-technies, says security expert Thomas J. Parenty.

Thomas J. Parenty is an expert on information security issues, has testified numerous times before the U.S. Congress on information security and global competitiveness, and is a consultant to many corporate and government organizations. He is also a gold medal-winning martial artist.

UBIQUITY: As you know, most of our readers are technical people. What would technical folks get from reading the book?

PARENTY: The technical folks would get the ability to communicate with the non-technical managerial folks about decision-making in the area of information security. When it comes to information security, business folks and IT folks speak separate languages. Business people have difficulty understanding the value to the organization of various security expenditures. Consequently, it is often difficult for IT folks to get the funding they need. One of my goals for the book is to initiate a common language between the technical and non-technical folks about how to make meaningful security decisions for an organization.

UBIQUITY: Why can't the two sides understand each other?

PARENTY: It is difficult for those two populations to communicate because of the gulf between general business objectives -- for example, increasing distribution channels, reducing customer service expenses, or pursuing a partnership for joint product development -- and security technologies. There's a void in understanding how technologies such as two-factor authentication, encryption of network communications, or firewalls serve the business objectives. Both populations should adopt an approach to information security that looks at security technologies, procedures and policies in the context of addressing, satisfying, supporting and enabling specific business objectives. It requires that the IT folks look at their jobs in more of a business oriented way than they have in the past.

UBIQUITY: Do non-technical managers take information security seriously?

PARENTY: My experience with many chief executives, senior VPs, down to directors, managers, and even individual contributors is that almost everyone will say that

information security is important. But when you mention viruses, firewalls and, heaven forbid, encryption, they almost faint. They have the perception that it's so difficult to understand security that there's no point in even trying.

UBIQUITY: How do you counter that perception?

PARENTY: My counter is that the amount of knowledge you need to make decisions about technology is much less than the knowledge you need to build it. Think about buying, let's say, a home theatre system. The amount of physics, acoustics and circuitry that are necessary to build a home theatre system is immense yet it is entirely irrelevant to the process of deciding what features and components you want. I'd like to see business decision-makers assume more of the role of home theatre purchaser and the IT folks to adopt more of the role of technical salesperson or enlightened friend who says, "If you want this sound quality, then you'll need to deal with those components." I'd like to see a collaborative working arrangement where it's recognized that the technical and managerial folks do not need to know the same information. But they need to be able to communicate with each other in order to be able to make useful decisions.

UBIQUITY: One of the principles mentioned in your book is, "Any effective corporate security process has to be closely linked to the specific business activities and mission of the company." Expand on that.

PARENTY: Even if I have perfect anti-virus protection, firewalls and intrusion detection, I cannot answer questions such as, is my customer financial information safe? Can my competitors get access to sales forecasting information? Are all of the checks cut by the accounts payable department for legitimate products and services that we actually receive? Anti-virus products and firewalls don't address how computers are used to support specific business functions. This is the area that I have spent most of my career on, which is, how do you incorporate security technologies into an organization's application systems?

UBIQUITY: Is there a conceptual difference between the kind of security that you would have to develop for an international company, such as Coca-Cola, than for, let's say, a railroad company or an airline?

PARENTY: Security issues are fairly constant across almost all kinds of business or government situations. It's good in the sense that there is basic commonality. However, depending on the specific organization, its policies, and how it is structured physically or organizationally, the ways in which you apply security technologies can be quite different. One thing I've realized in my work is that it is difficult to solve a general problem. The solution to a specific problem in a specific context is much simpler than trying to solve the problem for all circumstances.

UBIQUITY: When you have a client engagement at a company, with who do you normally deal?

PARENTY: I start with the folks at the executive level. I work with them on understanding the problem, and what the real risks and threats are. Then I work with folks lower in the organization to change things so that the organization is in a better position than before.

UBIQUITY: Speaking of change, what do you think has changed in the last 10 years in terms of information security in business? Are things getting better, are they getting worse, are they changing at all?

PARENTY: On the one hand, nothing has changed in that the fundamental problems that organizations need to deal with in terms of security are very much the same as they were 10 years ago. However, the number of different areas in which organizations now have to deal with those security issues has exploded, making things far more difficult.

UBIQUITY: What is the nature of the difficulty?

PARENTY: It used to be that, for the most part, computers were connected via wires to other corporate computers within a physically protected corporate campus. The amount of interaction with the outside world was relatively small. Today's environment includes the Internet and wireless networks. In addition to browser-based clients, you are communicating to PDAs, cell phones, and many different kinds of devices. The security issues are the same for each kind of network or device, for example, authenticating users and preserving the confidentiality of information as it is transmitted from source to user. However, now you have to use different security technologies and products to deal with these different environments. It is difficult to do.

UBIQUITY: Is it so difficult that some companies don't even try?

PARENTY: Many don't try and then there are companies that try but are undercut by their vendors. There's an example from the book of a company that produces enterprise software. Their wired browser base has user authentication and other prudent security measures. When they released a wireless version of the software for PDA access, the security measures were not included. I asked one of the lead engineers on the project about it. The engineer's response was, "That's not our responsibility. The users should take care of security for their PDAs." I asked, well, "If it was your responsibility in the wired world, why isn't it your responsibility in the wireless world?" He didn't have a good answer for why security was considered important in one deployment environment and not in another.

UBIQUITY: Do you think this was an exceptional case, or is it a fairly common attitude?

PARENTY: I know of many other cases of enterprise applications where this is true. And then organizations have even more things to worry about, like Internet chat and instant messaging. Internet messaging is yet another avenue into an organization that is not protected. The number of different areas in which organizations need to address security concerns is exploding. That could be a wonderful opportunity for security product vendors. But at the moment, it's a very large headache for those who are responsible for protecting corporate information.

UBIQUITY: You mentioned misunderstandings between business types and security types. Do you feel that security folks are regarded as happy warriors or as intimidating hangmen?

PARENTY: What is happening in the area of security is similar to a phenomenon that happened earlier in the area of medicine, in which doctors were perceived as all-knowing and powerful and who possessed a body of knowledge that mere mortals could never achieve. My perception is that the average person on the street views security specialists as folks who possess this body of knowledge that the average person can never understand and so there is no point in trying to participate in the betterment of one's security health. If somebody goes into a doctor's office, and the doctor says, "I think you need these invasive procedures. We can schedule surgery for next week," most people would say, "I would like to get a second opinion," or "I'll do research on the Web." The average consumer of medical services has a more active role in their own healthcare. Yet there is nothing in the area of computer security that approaches the complexity of the human body and its associated diseases. I am hoping that over time people will start to ask more questions of IT security folks such as, why is this necessary? What does this protect against? What am I still vulnerable to?

UBIQUITY: Your book talks about how security can be an enabler for business innovation as opposed to simply preventing bad things from happening. Tell me how.

PARENTY: When I was working on the book, I tried to find areas in which the right use of computer security technology would allow businesses to do things in a way that would be better in terms of economy, money making and logistics. In many business operations, there are limitations on how business activity or partnerships take place that are based on how security requirements are addressed. If we change those, we make things better in terms of business innovation. I'm talking about eliminating restrictions based on time, location and scale.

UBIQUITY: Can you give a specific example?

PARENTY: A contemporary example is the Hong Kong Jockey Club. The Hong Kong Jockey Club has thousands of employees taking bets at racetracks and off-track betting places throughout Hong Kong. Yet they realized that people were restricted by the need to go to one of those locations in order to place a bet. There is restriction on scale and also on locality. Through the issuance of digital certificates and private keys that reside in the SIM cards within cell phones, now people can place bets on horse racing, soccer or football from their mobile phones. They can do money transfers and other transactions making the Hong Kong national pastime of gambling much more convenient. The innovative use of security technology doesn't require brilliant insight. All it requires is that you look at an existing situation and then determine how to employ current security technologies to eliminate existing restrictions relating to time, scale and locality. It is useful for organizations to look beyond merely protecting themselves from a particular virus attack.

UBIQUITY: Let's talk a little about your background. You were a philosophy major at the College of the Holy Cross. Did you have a particular interest in philosophy?

PARENTY: Yes, I was interested in mathematical logic and Existentialism, but near the end of college I realized that I didn't want to be a cab driver or a bartender and so I decided to become a computer scientist. Studying philosophy under the Jesuits in terms of how to think and reason is incredibly useful in my field. My undergraduate training in terms of figuring out what is logically sound, how to make arguments, and what is required as a cause for some subsequent event was wonderful even though that wasn't my intent at the time.

UBIQUITY: Tell us what your specialties are.

PARENTY: Most of my career has been focused on evaluating and developing security for large complex systems. My first job at NSA was working on the design and evaluation of cryptographic and computer security technologies for protecting global nuclear command-and-control networks. More recently, I've worked on analysis and security architecture for global business-to-business trading. I have also designed security architectures for banking and healthcare applications and designed security features for products used by large enterprises. I come from a background with incredibly high, rigid security requirements. But I've also lived in environments with limited budgets, tight schedules, and the need to get something better now, even if it's not perfect, with an eye towards making it incrementally better as time goes by.

UBIQUITY: Why are you moving to Hong Kong? Are you going to spend most of your time in Asia?

PARENTY: I will maintain a US company and US clients but in general I will focus on Hong Kong, China, Singapore, Taiwan, Korea and Japan.

UBIQUITY: Do you have any employees?

PARENTY: I have contractors both in the US and Hong Kong -- I was going to say on "both coasts" -- that take care of administrative things. I also have a collection of consultants in the computer security and content management fields as well as lawyers and other folks that I draw upon as a particular client engagement needs it.

UBIQUITY: Are all security specialists also gold medallists in martial arts?

PARENTY: There is some overlap but not many of them run professional martial arts schools.

END

*Source: Ubiquity, Volume 4, Issue 36, Nov. 5 - Nov. 11, 2003
(<http://www.acm.org/ubiquity/>)*