DOI:10.1145/1859204.1859222

Article development led by acmqueue
queue.acm.org

**These days, cybercriminals are looking to steal more than just banking information.**

BY MACHE CREEGER

# The Theft of Business Innovation

## An ACM-BCS Roundtable on Threats to Global Competitiveness

VALUABLE INFORMATION ASSETS stretch more broadly than just bank accounts, financial-services transactions, or secret, patentable inventions. In many cases, everything that defines a successful business model (email, spreadsheets, word-processing documents, among others) resides on one or more directly or indirectly Internet-connected personal computers resides in corporate databases, in software that implements business practices, or collectively on thousands of TCP/IP-enabled real-time plant controllers. While not the traditional high-powered information repositories one normally thinks of as attractive intellectual property targets, these systems do represent a complete knowledge set of a business' operations. Criminals, who have come to understand that these information assets have very real value, have set up mechanisms to steal and resell them, bringing great financial harm to their original owners.

In this new world, businesses that may have taken five to six years of trial and error to develop a profitable model are targeted by bad actors who drain and distill operational knowledge from sources not traditionally viewed as highly important. They then resell it to a global competitor who, without having to invest the equivalent time and money, can set up shop and reap its benefits from day one.

In this CTO Roundtable, our joint ACM and BCS-The Chartered Institute for IT panel of security and policy experts discuss how the current threat environment has evolved and the implications for loss in this new environment. At stake is nothing less than the compromise of detailed operational blueprints of the value-creation process. The implications reach far beyond individual businesses, potentially to entire industries and overall economies.

*—Mache Creeger*

### Participants

**Louise Bennett**, chair, BCS Security Strategic Panel

**David J. Bianco**, incident handler, General Electric Computer Incident Response Team (GE-CIRT)

**Scott Borg**, director, chief economist, CEO, U.S. Cyber Consequences Unit

**Andy Clark**, head of forensics, Detica; Fellow, BCS; Fellow of the Institution of Engineering and Technology

**Jeremy Epstein**, senior computer scientist, Computer Science Laboratory, SRI International

**Jim Norton**, visiting professor of electronic engineering, Sheffield University; vice president and Fellow, BCS; chair, BCS Professionalism Board

**Steve Bourne**, CTO, El Dorado Ventures; past president, ACM; chair, *ACM Queue* Editorial Board; chair, ACM Professions Board

**Mache Creeger** (moderator) principal, Emergent Technology Associates

**CREEGER:** While past definitions have narrowly defined valued information as banking codes or secret inventions, criminals have broadened that definition to where they can clone entire businesses through the comprehensive theft of more mundane information such as manufacturing processes, suppliers, customers, factory layout, contract terms, general know-how, and so on. This new shift has significant implications to the competitive balance of entire industries, regardless of company size, and it has implications across the global economic landscape. How do you see this new security threat evolving, and how should businesses respond?

**BORG:** In 2004, when the U.S. Cyber Consequences Unit started, we were concerned about intrusions into critical infrastructure facilities, such as chemical plants and refineries. We believed that some of these intrusions were reconnaissance in preparation for an attack that would cause physical destruction.

We got that one wrong, because there were no major attacks of that kind. Further investigation indicated that when the attackers were in the control networks, they gave equal attention to equipment regardless of its ability to blow things up.

What they were doing was copying every bit of operational plant data they could get their hands on: how everything was connected, all the control systems, and settings for every pressure and temperature switch and valve across the entire facility. They were not stealing traditional intellectual property such as trade secrets or proprietary processes but the plant's entire operational workflow.

Soon after these attacks, new facilities in those very industries were popping up in Southeast Asia. No visitors were allowed, and we believe it's because they were exact replicas of attacked facilities.

From an economic standpoint, the degree to which you are ahead of your competition determines how much money you're going to capture from the market. The value reaped from being ahead is very dependent on your lead time as you develop your manufacturing facility. As a rule of thumb, when you open a new facility, you can reduce costs by 5% to 15% each year of operation for roughly the first six years. This amounts to a huge drop in cost, and for a lot of industries represents the majority of the profits. If someone can steal all the operational information it took you six years to develop and open a facility that on day one has the exact same level of efficiency, they have effectively stolen the majority of the profit for your facility.

Roundtable panel from bottom left: Jim Norton, David Bianco, Mache Creeger, Louise Bennett; top left: Steve Bourne, Scott Borg, Andy Clark, Jeremy Epstein, and BCS Director for Professionalism Adam Thilthorpe.

PHOTOGRAPHS BY MARJAN SADOUGHI

What is being stolen is something enormously more valuable than what has been lost to credit card or bank fraud. This is a huge issue and puts these companies and potentially entire domestic industries in jeopardy of survival.

**NORTON:** Should we assume that the attackers also lift one or two key staff people to help interpret this information?

**BORG:** If you take Asia as an example, using this type of information is often limited by the availability of people who understand Western business practices. This is not something you learn by taking a course locally. To use the information effectively, you have to send someone not only to study in the West but also to work in Western industry.

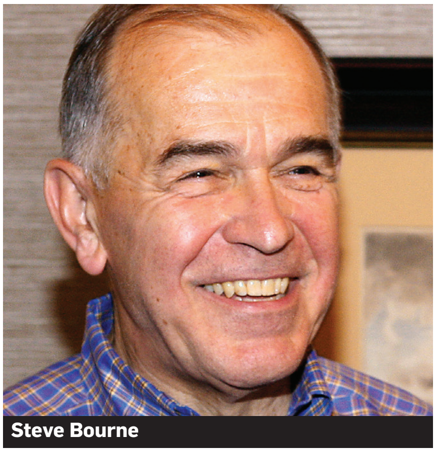
**BIANCO:** It used to be that you had to be just secure enough that an attacker would give up and go to a less-secure competitor. This is no longer true. Being targeted today means you have something of specific value, and the attackers will probably not go away until they get it. This is fundamentally different from past practices. The people who learned about this in January when Google made its Gmail announcement are probably several years behind everyone else.

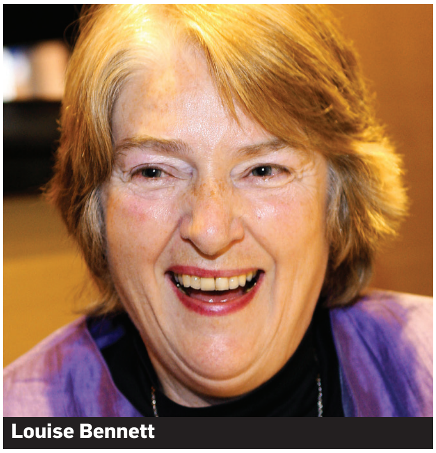
**CLARK:** Much of the business community looks at security as being the people who make sure all the doors and windows are locked. Rarely are security processes aligned with the business, but it's the business that drives security, and security should protect and support valued business processes. That's easier said than done.

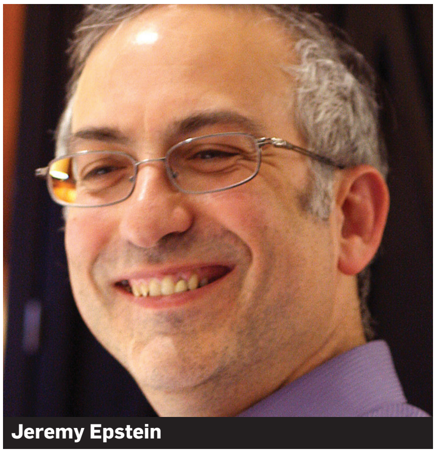
There is also the ethical dilemma of assuming that my competitor and I do business in the same way. That is clearly asymmetric, because your competitor may not follow your business rules. It's hard enough to run a business, be ethical, and work within your regulatory framework without an actor coming in outside of that framework.

We need to: (a) educate people that

Mache Creeger


Steve Bourne


Louise Bennett


Jeremy Epstein

there are others who work outside their business and ethical framework; and (b) define security as a function that works for you by supporting value-creating business processes.

**BENNETT:** One of the key considerations is motivation. The two main business-attack motivations are money/greed and reputation. People behave differently according to their motivation and the type of business they're attacking. Stealing factory operations know-how is different from stealing information about the pricing of a product that's about to be launched. Both of these are very different from destroying the competition by destroying its reputation.

As a business owner, you have to ask, "In what ways am I vulnerable in the electronic world? Who could attack me, why would they want to, and what would they want to do?"

**CLARK:** Is it the feeling around the table that industry is more sensitized to the confidentiality associated with cyber attack, rather than treating availability and integrity as equally important issues?

**BORG:** Companies are sensitive to the confidentiality of the information they designate as intellectual property. They are not as sensitive to the confidentiality of their control systems, their corporate email messages, or just about anything else they are doing. They do not appreciate the scale of the loss they can suffer from that other information being accessed by an outsider.

Jim Lewis (http://csis.org/expert/james-andrew-lewis) tells about a relatively small regional furniture company—not a business you think of as having key intellectual properties—that became an international target. This company had its furniture designs stolen by a Southeast Asian furniture manufacturer that went on to undercut the price.

If you look at your company from an attacker's viewpoint, then you can usually tell whether your company is a target and what specifically would be attractive. It is all about market-sector leadership, anyplace where the company stands out—for example, technology, cost, style and fashion, or even aggressive market expansion.

**CLARK:** Many of our adversaries play a very long game and do it very well. In the U.S./U.K. style of business we get caught up in quarterly or annual metrics and are not well educated in the long game. Are we naïve in not thinking more about the long game?

**BORG:** We have many people representing companies who are not properly incentivized to work in the company's long-term best interest. They are compensated on how they did that quarter or that year and not on whether their actions will cause serious crisis four or five years down the road.

**CLARK:** What advice can we give to IT managers and business leaders to mitigate these threats? Part of the answer is that we need broader education about the nature of threats and we need to understand the long game. I see the attacks on the furniture manufacturer as a long-game play. One waits until the target is ripe for picking, takes it, and moves on.

**CREEGER:** There is a lot of inertia to making changes in IT to address these issues. What suggestions do you have that would empower an IT person to say to management: "The survival and success of our business depends on you listening to my issues and acting on my recommendations."

**NORTON:** It has to be done through examples, and people don't want to publicize their attack problems.

**BORG:** My organization has been warned that we can tell these stories, but if we ever get specific enough that someone can identify one of these companies, then the executives of those companies will be sued by the shareholders, the executives will sue us, the supposed beneficiaries of the attacks will sue, and their business partners will sue as well.

**CREEGER:** How are we going share our collective wisdom?

**NORTON:** We can use the airline industry as a model. If you're a pilot of a plane that has a near miss, you can create an anonymous statement about what happened, when it happened, and so on.

**CLARK:** I can give an example of a breached business that was responsible for placing contractors in high-tech organizations. All of its data was based around individual CVs. An employee at that company chose to extract that data using a USB flash

PHOTOGRAPHS BY MARJAN SADOUGHI

drive and form a new business. The attacker waited until a contractor's previous engagement was coming up for renewal and then remarketed to the contractor under the new business banner.

In this attack, the techniques were very simple. To protect your business, you need to keep a close view of the people in the organization, their motivation and interests, make sure they are satisfied in what they do, and minimize the risk of them doing something criminal and damaging. The focus needs to move from being almost completely technological to a balance of social and technical.

**BORG:** A common delusion among high-tech companies is that their information has a limited shelf life because they are generating so much new information all the time. This leads to the conclusion that it doesn't matter if people steal information because it's almost immediately obsolete. From an economic standpoint this is just wrong.

**NORTON:** Let's presume that we can never keep these people out. How do we deal with that?

**CLARK:** This whole issue of information theft really isn't very new. These issues have been in play for hundreds of years. In our time, some things have changed, most notably pace and data volume stolen. The time necessary to undertake a successful attack has been reduced, and the volume of data that can be taken has dramatically increased.

**CREEGER:** Can we learn from other fields and experiences? On a previous security panel people talked about addressing the risk of malware infection along the same lines as public health. They said that malware attacks are like the flu. You are never going eradicate it and must live with some ongoing percentage of infections. It will be a different flu every year, and you can minimize your infection risk by implementing certain hygiene protocols.

**CLARK:** Many people design systems on the assumption they will always work perfectly. Often, auditing features are minimal, sometimes added as a later feature. We need to architect systems on the assumption that breaches will occur, so the functions needed for a proper response are readily available when it happens.

> “
> SCOTT BORG
> **There are five steps to follow to carry out a successful cyber attack: find the target; penetrate it; co-opt it; conceal what you have done long enough for it to have an effect; and do something that can't be reversed.**
> ”

**BIANCO:** You should assume all preventative controls will fail. While you still need prevention, you should put your new efforts into detection and response—both in mechanisms and personnel. When prevention fails, if you can't detect failure, you have a very large problem.

**CLARK:** In individual applications, we can quickly focus on technical detection without looking at readily available metadata—that includes other systems—that would dramatically improve detection. For example: "Did person A log onto a network? If yes, where was person A when he or she logged on? Does that match what the physical-access-control log reports?"

There is a very real danger that many vendors will provide a good but narrow view of your network and miss the larger context that states, for example, that a user was not supposed to be able to log in from an undetermined physical location.

At Detica we have found real value in mining substantial levels of contextual data that corroborate not just what's happening in the network but what was happening with the individuals that access the network at that point in time. People should not be lulled into a sense of false security because they have purchased a specific niche security product.

**CREEGER:** Are you saying that we have to start building a huge metadata infrastructure to determine if one event is consistent within a greater context? Who is going to write all these consistency rules that will flag events out of sync with expectations? Who is going to run all these services and on what platforms? How do we architect cost-effective solutions that expend additional cycles to monitor, audit, and determine to the second, third, fourth level whether the person's actually doing what's expected?

**BORG:** What you are describing as a problem is a huge opportunity. There are five steps you have to follow to carry out a successful cyber attack: find the target; penetrate it; co-opt it; conceal what you have done long enough for it to have an effect; and do something that can't be reversed. Each of these is an opportunity to stop an attacker.

Scott Borg

David J. Bianco

Jim Norton

Andy Clark

You can use these five steps to generate a comprehensive risk chart. By listing all the components of your information system such as hardware, software, networks, and so on, you can itemize the corresponding attack tools and their countermeasures. In this way you can produce a comprehensive security risk grid. Using this methodology to review various sites, we find that while attack tools are spread uniformly across the chart, defensive measures are piled into just a few areas. People typically put almost all their effort into penetration prevention and backup. Most of the other components have no defensive measure to offset defined threats.

We have a huge opportunity for the security industry to develop tools to do such things as quickly identifying bad behavior. Because bad behavior is highly specific to context and industry, security companies need to define industry-specific anomaly detection templates. I believe that is the only way that Andy [Clark's] issues will be resolved.

**BENNETT:** We have been looking at what I would call the positive side of the attack—that is, the attacker wants to *get* something. There is also an important negative side to an attack in which an attacker is trying to *destroy* something—whether it is reputation, data integrity, or the like. For me, destruction of digital assets is of greater importance.

**BORG:** The security industry has failed midsize businesses. They don't have the products they need, and they face challenges they can't meet. We have to provide them, either by national policy or security industry initiative, with better solutions than we have right now.

**EPSTEIN:** One role of government is to react and respond, but the other role is to regulate—to force companies to pay attention to these issues. For all the GEs in the world that are trying to do a good job addressing these issues, there are many more companies that do nothing because nobody is forcing them to do otherwise. In some cases they are independent software vendors selling poorly designed software that can cause future problems.

**BORG:** This is not an area that can be solved by governmental edict because the technology, including the attack technology, is changing so fast. When the government decides to force people, it has to decide what it's going to force them to do. By the time a standard is identified and regulators have begun enforcement, it not only will be obsolete, but also may very well be an impediment to implementing necessary measures. The best that government can offer is to help the market work better, by making sure there are adequate incentives, adequate product information, and other conditions markets need to function properly.

**EPSTEIN:** Government also provides the legal infrastructure that allows people to disclaim responsibility. If you buy any commercial security product, the vendor basically says that whatever happens, you are on your own. The ISVs take no responsibility for anything bad that happens.

**NORTON:** It's tempting to go down that route, but if you are not careful you could destroy the open source community.

**CREEGER:** Who is accountable? At the end of the day, someone has to stand up and say that this security product meets some reasonably well-understood, generally accepted security standard. For anyone going to a security-focused trade show, it is like a Middle Eastern bazaar of all sorts of competing product schemes.

**BENNETT:** The responsibility has to lie with the board of the company. One of the big problems, particularly in medium-size companies, is that they have been toddling along for a reasonable length of time and *n* generations of IT have happened while they've been operating. The challenge for the board of that company is to be educated as to what is really required to reduce the threat risk to an acceptable level for their industry.

**NORTON:** That is why the honey trap is so useful. If you can show that, despite existing protections, a company can still be penetrated, the board ought to be concerned.

**CLARK:** Many companies with a relatively young board and outlook don't care. They are much more focused on: "We need to do this work now. We are quite high paced and by the time the threat materializes, it's past and I'm not interested." They believe that their

PHOTOGRAPHS BY MARJAN SADOUGHI

business will last for a year or so and then they will move on. We need to be careful of the models we're using and should not claim them to be universal.

**BORG:** You can identify certain categories, and as you do so, you are also providing the business with clues as to what needs protection. If you are a cost leader, you have to think about what makes you a cost leader and try to secure those things. If you are a technological innovator but not a cost leader, you have a very different focus on what systems you should be trying to protect.

**CLARK:** Would it be fair to say that while the defense industrial base has been the prime target over the past 10 years, things are clearly changing now?

**BORG:** One of the real problems with this subject, with this whole field, is it's so hard to keep on top of it. Eighteen months ago, military contractors were overwhelmingly the leading target. That has now shifted to a host of other companies.

We are hearing about companies in South Korea, Indonesia, and other countries that are being offered business research services that will provide them with profiles of competitors and detailed advice on the state of the art in certain growth industries. Many of these research services are selling information they obtain through cyber attacks.

How does this marketplace work? Often there are black-market Web sites that offer the services and have customer reviews and satisfaction ratings.

**CREEGER:** Are there any concrete examples of industries being cloned?

**BORG:** Until relatively recently, the main organizations carrying out this kind of activity were national intelligence agencies. They were probably spending millions of dollars to steal the information from one of these target companies. They tried many, many generations of malware, as well as many different attack vectors. We now have privatization of these original efforts—spin-offs from the original national intelligence efforts working for hire.

We are talking about an illegal service—something that's not being sold as a one-off product. We're talking about a sustained business relationship where the customer starts out by buying information for a few thousand dollars (U.S.), becomes gradually convinced of the criminal organization's "integrity," and then goes on to make larger, more strategic purchases.

My organization has been theorizing about ways to subvert these criminal markets. Just as you can use cyber attacks to undermine trust and damage legitimate markets, you can use those same techniques, including cyber attacks, to undermine criminal markets.

**CLARK:** The structure of available worldwide attack services is broadly commoditized. You can pay using credit cards, not necessarily your own, to buy yourself a worldwide attack service.

> “ANDY CLARK
> **The structure of available worldwide attack services is broadly commoditized. You can pay using credit cards, not necessarily your own, to buy yourself a worldwide attack service.**”

**CREEGER:** We have learned that business sophistication and marketing in these criminal areas rival anything seen in the legitimate world. As an IT manager, what should I focus on in the next one to three years?

**BIANCO:** Focus on hiring people who understand how this stuff works.

**NORTON:** Get people to raise their eyes, look around, and ask, "What is unusual, and how was it caused?"

**BORG:** In addition, your company needs to be running Symantec, McAfee, Trend Micro, or another retail Internet security package. In many cases, it needs to be hiring the services of an intrusion-detection specialist.

Also, the company has to look at what it is trying to protect: "What are the attackers' motives, what are they going try to break into, what are they after, and what do you need to defend?" Basically, you have to answer the question, "Are you a target, and why?"

**CREEGER:** You're all strongly saying that the IT people need to be thought of as much more than just the people akin to supporting the plumbing, electrical, and telephone system. IT needs to take a much more integral role in the company's operations and contribute to how the company faces both challenges and opportunities.

**NORTON:** IT should be engaged in the business and understand how the business works.

**CLARK:** With regard to the urgency of this issue, I mentioned earlier that the pace of attacks has increased dramatically. Because in-place human assets are no longer required, the time needed to penetrate the whole of the industrial base is significantly less than it was in the 1980s. The man running his furniture business might not think he will ever be a target because he is ranked so low, but the attackers will get to him, probably sooner rather than later. We are in danger of thinking about this as a low-paced environment when the reality is it's high paced.

**BORG:** Cybercrime develops within predictable places. Typical markers are where you have unemployed people with a high level of technical training, where there is an ideological rationale for the attack—because criminals like to feel good about themselves—and where there is some kind of criminal organization to seed the effort.

As these pockets take hold, they often specialize in particular industries or even particular companies. So, a given, very famous, company will tell you that most of its attacks come out of a specific country. There is an opportunity for tampering with the ecology of the attackers and making their lives harder.

**CLARK:** At a minimum, all businesses should implement a basic level of protection using established commercial products and services. Even though there are many vendors in the market who deliver the basics and do it very well, many companies still do not have basic protection.

Then the next stage is to say, "I've done the basics. Now I need to understand whether I am in this next level and a target."

**CREEGER:** Given the current mantra of putting things in the cloud, does that make you more secure?

**EPSTEIN:** Yes and no. I would argue that for small companies and maybe even midsize companies, on balance, it's a good thing. For that sector, it is probably the first time that they're getting some level of professional management and some opportunity for the 24/7 monitoring they clearly need. For large companies, it's probably a huge step backward.

**CREEGER:** Because it's a one-size-fits-all security model?

**NORTON:** You have to have some basic quality criteria in the cloud providers.

**EPSTEIN:** You need to have a way for those small and medium-size companies to discern what type of security those cloud providers provide. A company I worked with outsourced its human-resources system, including all its sensitive employee information, to a cloud provider. I saw the administrator log in using a four-character password, and I said, "You know, this isn't a good idea." An employee, overhearing this, tried to log in with the stock ticker symbol, was successful, and was almost terminated for pointing out the vulnerability. The cloud provider should almost certainly shoulder some of the fault because it turned out that the policy was to accept a minimum of two-character passwords, even for the administrator account. The risk was increased because of the cloud, but the cloud provider was delegating the responsibility to the customer, who didn't have the proper expertise.

**CREEGER:** What I'm hearing is that the bad guys are way ahead because they're more innovative and profit driven. For the good guys, it's buyer beware, and you must really try to understand your business' realistic vulnerabilities. Always practice basic hygiene and look to the security industry for products such as intrusion protection, firewalls, antivirus, and the like. Don't count on that really bailing you out, however, if you are the target of a sophisticated and determined attacker.

The best advice is to recognize what makes you unique in the market and think honestly about how to protect those assets. This might include spending some money on a computer-literate consultant who could actually help you think through that process.

**BORG:** You have to guard against having the security consultant sell you a universal solution that promises to secure everything. You need to have a specific strategy that addresses your valued information assets.

**CREEGER:** Over time, the legitimate computer security world will catch up, and cloud service providers will have tiered certifications designed to fit the needs of specific industry sectors.

**CLARK:** Yes, but the threat will have moved on. We need to address the fundamental asymmetry of this issue. You will never catch up.

**EPSTEIN:** I want to add outsourced penetration testing as one more thing to be done. Penetration testing does not tell you where your problems are or how many problems you have but how screwed up you are. Gary McGraw calls it a "badness-ometer." Penetration testing is something that you can take to the board to show real risk and vulnerability.

**CLARK:** One needs to be cautious and balanced about the way those findings are presented. Penetration testers always find something. It is important that people understand the context of what is found, distinguish what is important in addressing the issues raised, and get to a known baseline. The computer industry should help educate people how their risk profile ranks with similar organizations.

**BORG:** Employees should never be told to protect valuable assets. If they're told this, they usually protect an object that may be expensive to replace but is not what creates or could destroy value. How value is created is a business' most important asset, and that is what people must focus their protection resources on.

**CREEGER:** Maybe a recommendation would be to take senior management to an off-site meeting and ask, "If you were a determined attacker to our business, what would you do to damage it or to re-create its value for some other set of shareholders?"

**BORG:** When we investigate the vulnerabilities of companies, we always get the engineers to sit down and red-team their own company.

**CLARK:** If you take a slice across the whole company and not just senior management, you'll get much more value. You need an entire cross section of expertise and viewpoints.

**NORTON:** It's not just about technology but a balance of people, process, and technology. There is intelligence at every level in your organization. The lower levels are often untapped and usually really understand where organizational vulnerabilities reside.

**BIANCO:** You have to have the right people on staff for this kind of effort. You need to deploy business-specific monitoring technologies and employ someone knowledgeable to look at the output of those systems.

Also, don't be afraid to talk to other

folks in your industry that are being exposed to the same threats. While they may be competitors on the business side, you all have a vested interest in lowering the industrywide threat level. The bad guys talk all the time. If you don't have industry-specific contacts, you will be at an even larger disadvantage. It's probably the least expensive thing you can do to increase your security posture.

**BENNETT:** Businesses need to understand an attacker's motivation to steal know-how, systems, and other assets. While the typical goal is to replicate and/or destroy the business, the protection of a business' reputation and the rigorous understanding of a business' vulnerabilities are not given the board-level visibility they require. New, young businesses actually understand this better than many medium-size, older businesses.

Attacks may not be just about money and may not be rationally motivated. A motivation for someone to destroy your business may not be "You lose, I win," but "You lose, I stay the same." Given the current state of the recession, that cannot be discounted.

**CLARK:** When things go wrong, you need to be in a position to understand what happened. That includes not just the technological side but the motivation side as well.

The IT security function needs to have a seat at the management table and directly align with the business' goals. I asked a CISO (chief information security officer) for a large multinational corporation about his objectives. He said, "My first objective is associated with contributing to the financial success of my business." That really focused his mind about the profitability and success of the organization and made him a critical player in the achievement of that goal.

**EPSTEIN:** Too many organizations spend their information-security resources on protecting their firewalls and other fairly low-level things such as the protocol stack. The activity these days is all happening in the application layer. While a lot of the small and medium-size organizations are just now getting around to protecting the bottom layer, the bottom isn't where the problems are anymore.

If you look at the nature of network attacks, Microsoft, Cisco, etc. have done a reasonably good job. Just because they have pushed attackers higher in the service stack, however, doesn't mean the game is over for us defenders. We have to move our defenses higher as well. We can't just monitor firewall logs anymore. We now have to monitor application logs, and a lot of applications don't have logs. While boards have been hearing the mantra of antivirus, firewall, etc., they now need to understand that the threat has moved up the stack, and the defenses have to move there as well.

I think the cloud is, on the whole, a positive thing. As computer scientists, we need to come up with a way to give users advice on how to select a cloud provider. We need the equivalent of *Consumer Reports* for cloud providers supporting specific industries, especially for small and medium-size businesses.

**CREEGER:** My take-away is that security is really tied up intimately with the semantics of your business. For a long time, most people have treated security with a one-size-fits solution, usually putting fences around certain critical components without thinking about the real semantics of operations. My impressions from our conversation is not only do IT people need a real seat at the senior management table so they can make substantive contributions to its profitability, but they also need to understand the company's long-term strategy and operations intimately in order to avoid calamity. C

> “
> MACHE CREEGER
> **The best advice is to recognize what makes you unique in the market and think honestly about how to protect those assets. This might include spending some money on a computer-literate consultant who could actually help you think through that process.**
> ”

**Related articles on queue.acm.org**

**Lessons from the Letter**
*Kode Vicious*
http://queue.acm.org/detail.cfm?id=1837255

**Intellectual Property and Software Piracy: an interview with Aladdin vice president Gregg Gronowski**
http://queue.acm.org/detail.cfm?id=1388781

**CTO Roundtable: Malware Defense**
http://queue.acm.org/detail.cfm?id=1731902

**Mache Creeger** (mache@creeger.com) is a technology industry veteran based in Silicon Valley. Along with being a columnist for *ACM Queue*, he is the principal of Emergent Technology Associates, marketing and business development consultants to technology companies worldwide.