

**InfoWorld**

GET TECHNOLOGY RIGHT

# THE PATH TO ENTERPRISE SECURITY

---

FEAR OF INSIDER THREATS HITS HOME **2**

---

COOL TOOLS FOR HACKER TRACKERS **5**

---

FORRESTER SECURITY SHOW STRESSES RISK MANAGEMENT **7**

---

ENTERPRISE SECURITY REMAINS A BALANCING ACT **9**

---

HOW GREAT IT SECURITY LEADERS SUCCEED **11**

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).

COMPLIMENTS OF

**NOKIA**

# FEAR OF INSIDER THREATS HITS HOME

**IT SECURITY TECHNOLOGY SOAKS UP A LOT OF THE SECURITY BUDGET, BUT COMPANIES ARE STARTING TO SEE THAT THE INSIDER THREAT POSED BY EMPLOYEES IS JUST AS IMPORTANT. BY MATT HINES**

**T**he more money that companies spend on securing their IT operations from external attack, the more it seems they become aware that the potential threat posed by their own employees remains their most significant risk.

A new study published by consultants Deloitte on Tuesday finds that financial services companies – among the most advanced and deep-pocketed consumers of security technologies in the world – are still struggling with the concept of handling the insider threat issue despite all the cash they’re dropping on security technologies.

In the survey of 100 global financial services firms, Deloitte found that 91 percent of those questioned were concerned about their inability to respond to insider threats, while 79 percent were willing to cite “the human factor” as the root cause for a majority of their security issues.

Despite that and all the different types of security tools companies have adopted, the survey found that 22 percent of the companies interviewed hadn’t provided any new security training to their workers in the past year, and only 30 percent indicated a belief that their current employees were skilled enough to respond to an emerging security crisis.

The apparent lack of faith in their ability to control the insider threat shows that many businesses are aware that they are only just beginning to tackle the problem, report authors said.

“The contradictory findings highlight the security paradox financial institutions are facing,” Mark Steinhoff, leader of the firm’s financial security and privacy services practice, said in the report. “Security training and awareness, along with access and identity management—of employees, clients, and suppliers alike—are among organizations’ top initiatives this year as they fight to keep pace with the ever-changing threat landscape.”

Beyond training, more companies are also enlisting the help of additional security systems aimed specifically at thwarting internal attacks and preventing mistaken data breaches.

In addition to tools that offer the ability to track IT systems usage more comprehensively – and create electronic paper trails that give forensics experts a string of clues when investigating any misbehavior or mistake – enterprise organizations claim that they are also blending physical and IT security to stay abreast of what their workers are up to.

“We’ve been putting cameras on all entrances and exits, looking at using badge numbers for tracking purposes, and keeping a closer eye on what people are doing and where they are going,” said Adam Le, director of IT infrastructure at Alliance Imaging, a healthcare testing specialist. “We’re also contemplating things like fingerprint scanners and other biometrics and looking at encrypting all data at rest on laptops.”

Companies walk a fine line in balancing the need to watch over their

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).

## ANALYSIS: FEAR OF INSIDER THREATS HITS HOME

workers for security purposes and becoming too intrusive, the expert admitted. However, Le said that with businesses like Alliance facing mounting pressure from regulators to lock down every piece of patient data they record, employees must understand that the process is about protecting the firm and not about assessing personal work habits.

In another effort to deal with the insider threat, Alliance, which provides outsourced medical imaging capabilities to hospitals and other healthcare organizations, has added new user authentication and monitoring tools made by ConSentry to its IT environment.

By increasing security for remote workers and giving the firm a more detailed roadmap of file access activities carried out by its employees and customers, Le said he believes Alliance is finally getting ahead of the insider problem and arming itself with a way to keep everyone honest.

One of the most significant issues the company has dealt with in the past are efforts by insiders to view the records of famous or high-profile patients, activities that are directly at odds with the Health Insurance Portability and Accountability Act medical data protection regulation.

In some cases, the incidents have been the result of mere nosiness, while in others, the firm suspects that workers may have been looking to share sensitive data with outsiders for a profit.

After conducting both technological and physical penetration tests on its operations, Le said that Alliance feels it is making the right moves to address the issue after augmenting its operations as such.

“With the threat of data theft for identity fraud or to get information on our high-profile customers, we had to work to get a better picture of who was accessing what files,” said Le. “Since putting the tools in place, we’ve been able to track people down when they do something wrong, and I think that type of response travels among workers by word of mouth; overall those types of issue have almost disappeared now that people know that their activities will be monitored.”

### DATA LEAKAGE PREVENTION TOOLS BECOME MORE POPULAR

Another angle on preventing insider data breaches is being pursued via the use of so-called DLP (data leakage prevention) tools.

At WebEx, the well-known online conferencing applications vendor, Security Engineering and Operations Manager Mike Machado said that the company is using advanced DLP technologies made by Reconnex to ensure that workers aren’t walking out of the building with the company’s next big idea.

“Up until now, we didn’t have anything in place that could capture everything that goes over the wire, but the ability to use technology do to do this type of testing, versus doing sampling in the past, has given us a much clearer picture of where data is going on the network and who is touching it,” Machado said.

“Most of the incidents we find today are people unaware of policies, it’s only occasionally that we find something malicious, but typically the result is a simple behavior discussion, and that’s helping people expand their own understanding of what they should or shouldn’t do,” he said.

Another advantage to using DLP to keep an eye on all the data being transmitted out of WebEx’s network is that the tools serve as another proof point to show external auditors when those groups are testing to see if the firm is employing comprehensive information protection.

Perhaps the best use case for the technology yet, however, is when WebEx used the tools to catch an employee attempting to participate in a malware-distribution ring.

In addition to joining sides with the malware gang, the employee had also agreed to allow the group to use excess WebEx network capacity to harbor potential attacks – a problem that would have reflected poorly on the entire company if it were discovered and publicized, said the expert.

“It’s taught us that a lot that goes on that we know didn’t about and verified things we suspected. Overall, it’s been a valuable tool for detecting problems and putting us in position to prevent bigger problem down the road,” Machado said. “In the rare case we find something to

-----  
“In the rare case we find something to investigate, the technology gives us a much more credible case.”

•  
**MIKE MACHADO**  
**SECURITY ENGINEERING**  
**AND OPERATIONS MANAGER,**  
**WEBEX**  
-----

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).

## ANALYSIS: FEAR OF INSIDER THREATS HITS HOME

investigate, the technology gives us a much more credible case.”

The tools have also proven useful for helping the WebEx 's IT security team closer ties with the company's traditional security unit, which has helped the firm coordinate efforts to look for suspicious employee user behavior and policy violations.

“Because we were able to help them shed light on some valuable issues, the technology has really closed the loop in that sense,” Machado said. “The relationship wasn't always very good, but now, they're willing to be more forthcoming with us, and we can rely on each other more to reach our common goals, which is a big advantage.”

Some experts contend that companies will spend the next several years loading up on technologies that can help control insider threats now that they have invested so heavily in network defense protections.

Brian Contos, chief security officer at ArcSight, an IT security management specialist, said that businesses must consider the insider

problem as a dynamic, ever-changing issue, much like protecting against malware, if they hope to stay ahead of major incidents.

“The network security side of things has increased at a much faster rate, but it's still the Wild West to a certain extent inside many large companies when it comes to protecting applications, databases, and other systems with a lot of rich data stored in them,” said Contos, who previously authored the popular insider threat tome *Enemy at the Watercooler*.

“To be successful, you can't ever be more concerned with internal or external threats. In reality you have the very real chance for either type of attack on a daily basis,” he said. “The vast majority of employees, almost all, are not malicious, but you have to constantly watch for that one person who obtains employment deliberately to cause harm or who becomes disgruntled and decides to use what they know against you.”

-----  
*Matt Hines is a senior writer at InfoWorld.*

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).

# COOL TOOLS FOR HACKER TRACKERS

**A HONEYNET REPORTING SITE AND THE LATEST VERSION OF A SOLID HACKING PACKAGE HELP SECURITY PROS BY ROGER A. GRIMES**

If you want to keep up with the latest criminal exploits without having to collect malware yourself, take a look at SRI International's Cyber-Threat Analytics BotHunter Malware Analysis Web page. Reporting on information and statistics collected from a research honeynet, the BotHunter Malware Analysis page makes daily infection logs from high-interaction honeypots available for anyone to view. Although the scale of the project and information collected is fairly small, this is a useful site for gaining more insight into crimeware and the world of bots.

Clicking on any of the daily reports presents dozens of pieces of information on each day's attacks. It starts off with time and date of each bot attack, and the honeypot platform type (e.g. Windows XP, Windows 2000, etc.). It reveals the Snort rules used to detect incoming malware and how many antivirus companies detected the malicious code.

Each captured malware program is run against 28 to 32 antivirus engines. Try browsing the daily reports to see how many times none of the antivirus scanners detected the malware. Surprisingly, this happens roughly one third of the time – not a comforting statistic.

The honeynet automatically extracts plain text strings and tries to determine which executable packer was used. It decodes each executable and provides code traces. It appears that complete assemblies and packet traces are available upon request. A short summary forensic log

can be obtained for each malware attack. Here's a sample:

**FORENSIC LOG:**

**Infection Source:**

24.64.x.x

**Executables Delivered:**

ftpupd.exe

keymmuda.exe

**Listen Ports Opened:**

4166

4606

**Processes Created:**

keymmuda.exe

MSMSGSEX.EXE

**Registry Entries Modified or Created:**

HKEY\_LOCAL\_MACHINE@...Microsoft\Wireless

**CAIN & ABEL UPDATE**

Like many leading-edge technology companies, one of my favorite hacking utilities, Cain & Abel, is constantly updating itself. For years it's been the hacker utility with the most built-in features of any GUI tool. It can crack at least 28 different password hashes, conduct ARP

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).

## SECURITY ADVISOR: COOL TOOLS FOR HACKER TRACKERS

spoofing and man-in-the-middle attacks, and sniff more than a dozen different passwords off the wire. When converting password hashes to passwords, it can use several different cracking methods, including dictionary, brute force, and rainbow tables. It's not the fastest (get John the Ripper for that), but it's the easiest and most versatile tool available. The program's single downside is that it is only available for Windows.

I've been aiming to test Cain & Abel on Windows Vista since Vista came out almost a year ago. Although Cain & Abel must be started in elevated mode, many of the key features don't work, as I suspected might be the case. Protected Storage, RDP, and Credential Dumper didn't work, although a local LSAdump of custom service account passwords and wireless preshared keys and hashes did. I couldn't get any of the man-in-the-middle attacks to work, and none of the tools for sniffing passwords off the network provided any usable data.

I was happy to see that the local password hash dump only discovered the harder-to-crack NT hashes with no super vulnerable LM hashes available. This reflects Microsoft's decision to finally disable LM password hashes by default in Vista, a decision overdue by at least five years.

Some security administrators ask me why I promote the use of tools

like Cain & Abel that make hacking so easy. Shouldn't I be afraid of putting dangerous tools into the hands of the script kiddies? My reply is always the same: Hackers don't need Cain & Abel. They can do what they need to do without the easy-to-use GUIs. Cain & Abel is for the rest of us to make hacking easier to demonstrate. One good Cain & Abel demo to management can say more than a hundred computer security articles. And besides, most malicious hacking today is done by professional criminals ... and they don't use Cain & Abel either.

I often encourage system administrators to run Cain & Abel, with appropriate permission of course, to ferret out weak and plain text passwords on their own local system and on their networks. Most first-time users are surprised to find that plain text passwords abound on networks they believed were relatively secure.

Who am I kidding? Every system administrator I know thinks their network is like Swiss cheese. But Cain & Abel gives you a way to document the problem, and to begin doing something about it.

-----  
*Roger A. Grimes is contributing editor of the InfoWorld Test Center. He also writes the Security Adviser blog and the Security Adviser column.*

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).

# FORRESTER SECURITY SHOW STRESSES RISK MANAGEMENT

**ENTERPRISE SECURITY WORKERS ARE STARTING TO WARM TO THE CONCEPT OF COMPREHENSIVE IT RESTRUCTURING INSTEAD OF SIMPLY ADDING NEW TECHNOLOGY TO THE FOLD BY MATT HINES**

**E**nterprise security decision makers have long been more likely to be swayed by flashy new technologies than by the notion of comprehensive IT restructuring to protect data and other corporate assets, but the situation is evolving rapidly, according to experts participating in Forrester Research's ongoing Security Forum.

Kicking off in Atlanta on Sept. 5, the two-day event will bring together a number of influential IT security consultants and researchers along with a range of vendors and end-users to debate pressing issues impacting enterprise businesses today.

Whereas such technology meetings, including Forrester's inaugural 2006 security confab, have historically focused more on the acquisition of new technologies or the latest trends in malware, companies are finally beginning to spend less time on investigating individual attacks and defense mechanisms and more closely examining the idea of broad-ranging risk management, show organizers said.

"There isn't any hot new technology being pitched at us these days. The process is less about shiny widgets than it is about cohesive programs that combine security and risk management," said Laura Koetzle, the Forrester analyst charged with pulling the event together.

"For a long time, the power in the security industry has been in the

hands of the technology providers," she said. "But as enterprise security programs are maturing, we're seeing a shift to more coherent strategies that emphasizes specific business needs."

Koetzle said that the annual conference will have its fair share of security research reports on emerging threats – including the latest on messaging security trends from specialists with Postini – but the analyst highlighted increasing sophistication of the planned discussions, which focus on how companies can work with their customers and business partners to take a more organic approach to security.

"Many people growing up in the security discipline have seen a lot over the last few years, and now they're focused on working with business partners both inside and outside of their firms to get a more holistic view of what they want to accomplish, versus blocking viruses and filtering," said Koetzle.

"Today, security folks are much less likely to be a guy in a black hat in charge of some esoteric technology whom you never see, it's more about people who coordinate management strategy for companies and ensure that they have the right skills and partners in place," she said.

The Forrester analyst contends that security professionals are also no longer forced to fight for attention among the ranks of IT with c-level corporate leaders having woken up to the fact that their companies'

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).

## ANALYSIS: FORRESTER SECURITY SHOW STRESSES RISK MANAGEMENT

operations and reputations can be severely affected by data breaches and security gaffes.

Among the scheduled speakers at the show will be representatives from IT vendors including Dell, Texas Instruments, and VeriSign, but Forester has also corralled customers from the financial services and healthcare industries to share their latest experiences.

Along with a slew of Forrester's own experts, academic researchers from Johns Hopkins University and Purdue University are also slated to speak at the show.

Representing Johns Hopkins will be Dr. Aviel Rubin, director of the school's Information Security Institute and a well-known expert regarding e-voting technologies and many of the issues that loom with the continued adoption of the systems.

Rubin, who will also be representing his Baltimore-based consulting firm, Independent Security Evaluators, said that he will explain to show attendees how many existing IT products can still be broken by sophisticated hackers.

"It will always be a fact of life that things can be broken and not always by the good guys who will publicize it, so it's important that people examine the way they handle incidents, and it's always good to encourage people to share their stories," Rubin said.

However, the researcher said he will also focus on the process improvements that many companies have been able to appreciate as their

security efforts have matured.

"With the experience they've accrued, some companies, including vendors, are doing a better job of handling vulnerabilities and reporting," he said. "However, it's still useful to look at how things can still be circumvented and look at the measures that are being put in place to stop that sort of activity."

Also presenting will be Brian Contos, chief security officer at security management specialists ArcSight and the author of the well-known insider threat tome *Enemy at the Water Cooler*.

Contos agreed that the political battles that IT security pros needed to fight just to get attention and budget from business leaders have waned over the last several years and said that companies are getting far more aggressive in how they police their users and networks.

However, that shift has also created new challenges, he said.

"People want to monitor almost everything, but by adding more events, they are moving from megabytes of result information to terabytes and also trying to meld IT security efforts with physical security, which will be a long process," Contos said. "The main question we're hearing has become how companies can deal with this flood of data and turn it into something valuable, that's the challenge that many of these enterprise customers face going forward."

-----  
*Matt Hines is a senior writer at InfoWorld.*

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).

# ENTERPRISE SECURITY REMAINS A BALANCING ACT

**MINIMIZING RISK BY IMPROVING PROCESS, PRIORITIZING THREATS, AND ACCEPTING LIMITATIONS IS THE ONLY WAY FOR LARGE ENTERPRISES TO EFFECTIVELY DEFEND THEIR OPERATIONS BY MATT HINES**

**T**he sheer size and complexity of today's largest enterprise businesses makes it nearly impossible for such organizations to keep up with the rate of change in IT security, requiring a top-down strategy that prioritizes risk and accepts the limitations of available technologies, according to a top executive at financial services giant Morgan Stanley.

Presenting to the assembled crowd at the ongoing Usenix Security Symposium in Boston on Thursday, Jerry Brady, global head of IT security at Morgan Stanley, painted a bleak picture of the situation faced by large enterprises in trying to balance defense of their computing systems with keeping operations up and running to support business activities.

From the challenge of finding software developers who understand the security implications of their work to studying the geopolitical forces at play in all of the corners of the world in which Morgan Stanley does business, Brady said that his company's efforts to lock down IT systems are almost constantly in flux.

Only through the adoption of high-level policies and controls aimed at fostering flexible security practices across the organization and via more aggressive sharing of information about threats with other businesses – and law enforcement agencies – can large companies effectively improve their protection and continue to do business as usual, he said.

Keeping up with all the product security patches issued by mainstream

IT providers and adopting all the latest systems defense technologies are impractical tactics for companies like Morgan Stanley, which employs roughly 70,000 people worldwide and controls roughly 100,000 different computing devices, Brady said.

Establishing a strategy that involves near constant refining of security policies, includes heavy amounts of research into emerging threats, and is built around assessment of how any IT work might impact business operations is the key to balancing the entire equation, he said.

At the end of the day, the notion of making an enterprise completely secure from attack is impossible to achieve based on the scale and diversity of the systems employed by such companies and the multitude of threats they are dealing with, according to the executive.

"Depending on the theater of operation or part of the company you're looking at, you will find incredible degrees of variety in terms of the security that's being required," said Brady. "We try to pull this together into something that works by using a policy-driven, versus technology-driven, approach that establishes security controls that people can localize."

Adding another degree of complexity to the issue is the near constant rate of mergers and acquisitions carried out by companies like Morgan Stanley with each individual firm bringing their own specific IT footprint into the larger picture, including whatever technologies they have chosen

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).

## ANALYSIS: ENTERPRISE SECURITY REMAINS A BALANCING ACT

to use, said the executive.

The notion of patching every Windows system in the company after Microsoft issues its monthly Patch Tuesday security bulletins is impractical for reasons related to asset logistics as well as the need to keep IT systems up and running to support Morgan Stanley's internal users, partners, and customers, he said.

"All of these factors are what turns this into a centralized risk management process where we also look at the area of the world and specific operational risk in making decisions about managing security," Brady said. "Issues of uptime make it so that we don't have realistic windows for patch management; it's unlikely that we're ever going to get a window to manage security like the manufacturers thought we were."

### LOCAL SOLUTIONS FOR GLOBAL BUSINESSES

All of the various data privacy regulations that the financial services firm faces around the globe are yet another reason why the company has to create broad security policies that can be tailored for local environments.

While many countries have national policies for protecting customer or financial data, for instance, the United States has decided to let each state handle the issue on their own for now, making it even more important to take a top-down process-driven approach, Brady said.

In some cases, the company finds itself at odds with malicious efforts being carried out by the foreign governments themselves, particularly in the Far East, he said.

"Sometimes the threats are coming from the governments themselves in different parts of the world, whereas in North America, our retail organizations are dealing with specific types of attacks like pump-and-dump schemes," said Brady. "As such, the controls need to be very different, but it all comes together in a model where we take into account information security, data security, regional risk, and physical security in one big picture that can be difficult to coordinate, but we try to do so through strong process and procedures."

For instance, while the top security priority in one nation may be preventing sophisticated hackers from breaking into the company's electronic trading

systems to steal the unique algorithms used to maximize returns for its customers, in another location, the biggest fear might be attackers who might attempt to break into physical offices to steal hardware or sensitive records.

One of the biggest issues facing financial services companies today is the matter of protecting their internally-developed business applications, which for decades have been built with time-to-market issues considered first and security considered only after they go live, the executive admitted.

However, Morgan Stanley feels that the best way to address the problem

is to aggressively re-train its developers and build secure coding processes into its software development lifecycle in a comprehensive manner – rather than investing heavily in all the code and applications security testing products that are currently being brought to market, he said.

Brady contends that one of the most effective weapons that enterprises have gained in the past few years that is helping to manage the overarching security issue is a greater sense of cooperation between businesses – particularly those in the financial services arena – as well as law enforcement agencies in sharing information about new attacks or adversaries.

Whereas only several years ago companies were reluctant to share details of what they were experiencing, businesses have learned that they can help themselves by aiding each other, the security expert said.

"The people who want to harm us drive a lot about how we think of security awareness. We do a lot of

monitoring and threat intelligence to tell who our adversaries are today and who they will be tomorrow," said Brady. "As such a large company, we can't really make infrastructure adjustments quickly, so, we need to understand a lot about the people who want to hurt us and do long-term planning."

"Understanding the underground requires a lot of work with law enforcement and our competitors, and historically this hasn't worked out too well," he said. "But over the last several years we've started sharing data in real-time, and if one of us gets attacked, the rest of us know the details quickly; this sort of an approach is so much more effective than one that is directed by the use of technology."

-----  
"Sometimes the threats are coming from the governments themselves in different parts of the world, whereas in North America, our retail organizations are dealing with specific types of attacks"  
•

**JERRY BRADY**  
**GLOBAL HEAD OF SECURITY,**  
**MORGAN STANLEY**  
-----

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).

# HOW GREAT IT SECURITY LEADERS SUCCEED

**FORRESTER IDENTIFIES SOME SURPRISING ATTRIBUTES THAT MAKE FOR THE BEST-PERFORMING CISOs BY MATT HINES**

As the threat of attack, both external and internal, continues to take root and as data-handling regulations continue to proliferate, the role of a chief information security officer appears to be growing more complex by the day. Many CISOs are doing an admirable job of stemming the tide of data loss and keeping their heads above water around compliance. But some IT security leaders are doing it better than the rest, according to a recent Forrester Research report, which has identified several characteristics that make these top CISOs more successful than their peers.

Beyond predictable recommendations such as having a close relationship with their employer's business leaders and making security a pervasive issue across their entire organizations, several unexpected practices arose during Forrester's discussions with users, vendors, and regulators.

## **A MORAL COMPASS IS THE KEY TO SUCCESS**

The top finding was that truly effective CISOs must have a strong moral compass that allows them to lead as much by example as they command respect via mandate. "CISOs are expected to have a certain level of technical skill, but the character of the person really drives a lot of the success that they might have in this position," said Khalid Kark, a Forrester analyst and the report's chief author.

"Having the integrity, the visibility, and letting people know that you as an individual will always do the right thing is of great importance when you are being trusted to protect a lot of sensitive information." Other C-level executives may be able to get away with taking sides in corporate standoffs or going behind people's backs to accomplish their goals, but CISOs who expect to garner the level of respect needed to carry out their jobs most effectively must emit a persona of undeniable trustworthiness.

"Before doing the research, I wouldn't have guessed how important this aspect might have been, even having managed security operations myself," said Kark. "But it became clear that this is a characteristic that many people really value in a CISO. One of the issues that these executives face is that it takes time to build trust, and if you have that [moral] compass where you instinctively know what [is right] to do, you can achieve that [trust] in a shorter timeframe."

Also important to gaining that trust and executive buy-in is an ability to work with "the corporate psyche," as well as balancing the CISO position's political and policing roles.

Other key attributes of the most successful CISOs include having the flexibility to look for creative solutions to problems and move quickly from one project to the next, remaining patient whenever possible, and running security as if it were a business unit. That latter talent requires

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).

## ANALYSIS: HOW GREAT IT SECURITY LEADERS SUCCEED

the ability to gather important security and compliance data, plus knowing how to use it to defend related budget items and project work.

One of the most important assets for any CISO, Kark said, is to behave as a “kingmaker,” someone who helps other people improve their own skills by acting as a mentor, rather than as a draconian ruler who merely gives commands and expects them to be followed. “CISOs need to help other people succeed and take over different responsibilities. This should be part of their overall security strategy,” he said.

A related talent is not playing the blame game. “CISOs also have to be willing to take on a lot of the blame when things go wrong, even if it was someone else’s fault. You don’t want to take the blame for everything, but if you can stand up for someone else’s mistake and use that to work on issues that improve the overall position of the organization, that’s a great thing to do.”

### VALUE OF DEEP TECHNICAL SKILLS IS QUESTIONED

One aspect that the Forrester report did not cite as critical to a CISO’s success was having a high level of technical skills. “Some people said

yes, and others said no. This is an old debate,” Kark said. “I think the key is that you absolutely need to have the ability to comprehend technical data, but you don’t necessarily need the hands-on skills. Many successful CISOs don’t focus on operational issues like managing firewalls, but they do need to be aligned with defining security policies and crafting the risk posture of their organization.”

In fact, many CISOs who do have technical skills contend that the knowledge often leads to them getting tied down in too many operational decisions and projects, he said.

Regardless of a CISO’s technical abilities, Kark said that it will become increasingly important for security leaders to move away from a bottom-up approach to security, where the focus is what tools to use, to a top-down approach driven by risk management and governance concepts. “These executives need to move from operational expertise into more of a role of a strategic thinker, from a policeman to a trusted adviser,” he said. “They need to see themselves more as a consultant, as opposed to an auditor, and transition from a specialist in IT security to a generalist in overall business risk.”

See the full selection of InfoWorld IT Strategy Guides at [http://www.infoworld.com/ad/sponsored\\_resources.html](http://www.infoworld.com/ad/sponsored_resources.html).