InfoWorld DeepDive

How to rethink security for the new world of IT

NOT ALL THE PROVEN PRACTICES OF THE PAST WORK IN TODAY'S INTERCONNECTED, HETEROGENEOUS WORLD.

HERE'S WHAT YOU NEED TO DO DIFFERENTLY.

Deep Dive

How to rethink security for the new world of IT

Not all the proven practices of the past work in today's interconnected, heterogeneous world. Here's what you need to do differently

BY BERNARD MATHAISEL, TERRY RETTER, AND GALEN GRUMAN

The fight for security is harder than ever. Most organizations are fighting today's war with yesterday's tools and approaches — and losing.

"We shall fight on the beaches. We shall fight on the landing grounds. We shall fight in the fields and in the streets. We shall fight in the hills. We shall never surrender," said Winston Churchill in his famous June 1940 speech in the face of Nazi attacks on England. His earlier committment to the goal of victory, "however long and hard the road may be," is an apt analogy to the security battles that enterprises face.

The bad guys are persistent, sophisticated, and they are making inroads. It is hard to be optimistic when customers, investors, and regulators expect us to totally protect precious assets and preserve privacy, while some governments and vendors on whom we depend are themselves compromising our data, software, and networks.

The fight for security is harder than ever. Most organizations are fighting today's war with yesterday's tools and approaches — such as protecting perimeters with passwords and firewalls — and losing. There is too much emphasis on walling off our data and systems, and a misplaced belief that the secured-perimeter approach is adequate.

We've talked to dozens of security experts, industry experts, and business executives to come up with a better framework for security today. What follows is that framework.

Focus on risks and people, not just devices and data

A much better defensive approach is built around a risk mindset. Yes, a key risk is the loss of critical or sensitive data, so you must adequately protect data. However, there are other risks, such as disruption of business operations, damaged reputations, regulatory noncompliance, investment risks, and intellectual-property loss. Which of these dangers could most hurt you? How do you assess threats? How would you protect against those threats, from greatest to least impact? Perimeter protections often don't address these concerns.

For example, credit card processor Visa International undertakes a full risk assessment of all its processes, including — but not only — where technology supports those business processes. "Risk is where a vulnerability meets a threat, and taking a holistic view of risks is the basis of a solid approach to security," says George Totev, former VP of information security, governance, risk, and compliance at Visa.

In essence, assessing risks is what you do when you buy insurance. When you buy insurance, you (or at least your insurer) are thinking about vulnerabilities that lead to bad consequences.

Risk assessment and risk protection vary by industry and enterprise. Some require the use of technology, some require process change, and others require changes in people's behavior. Other organizations are forced to address some forms of security risk because of regulation, regardless of their own risk analysis. Their focus becomes about meeting the requirement effectively and without an undue burden on their operations, finances, or strategy.

Whatever a company's risk philosophy and

Deep Dive

A security strategy for today must change the primary defense emphasis from devices to people.

its outside requirements, being selective and focusing on the highest risks is the practical approach.

But how to focus on those risks? Most companies — as well as the security vendor industry — treat security as a technical challenge. They seek to have software, hardware, and services identify and reduce the risks. Few involve their people — the very folks who create and use the information that is being protected. Many organizations actively exclude their people from their security approaches because they do not trust people.

There is no technology silver bullet for security, and automating people out of the security equation has the perverse result of making people lazy or uncaring about security. After all, IT will take care of it, and take the blame when there's a leak or breach.

That's why a security strategy for today must change the primary defense emphasis from devices to people. The key successful attacks today involve people, whether those using social engineering methods such as phishing to physically putting interception hardware on automated sales terminals.

Security is a dynamic game of risk relativity — namely, are your defenses better than the current level of threats? The words "dynamic" and "game" are both relevant. Security follows the laws of entropy: The energy levels will run down if not renewed. Constant vigilance is required. And a gaming mindset is crucial to keep the vigilance both active and adaptive. After all, each new defense is challenged by a new trick. People are naturally good at this, and you should be engaging your people to tap into that human ability, not automating them out of your defenses.

You need to get into the mindset of the people who create the threats. They're gaming your employees; you need to game them — and your employees need to be active participants as your eyes and ears, not blinded users.

In other words, stop treating your people as a problem to contain and instead begin making them part of the solution.

Five dimensions of the new security model

Although you're years away from perfection, enough plausible patterns have emerged to let businesses begin the necessary adjustment. The new model is additive. You must continue the best practices you have employed in the highest areas of risk, while incorporating the risk and people orientation of an improved defense.

The new model has five dimensions:

1. Narrow the information security focus to core, critical assets.
2. Protect key assets with multilayered defense systems.
3. Engage the people who use information to protect the assets they work with.
4. Team with business partners to boost their (and your) immune systems.
5. Make security a business problem — not just IT's problem.

1. Narrow the information security focus to core, critical assets

Perfect security is impossible. Yet protecting everything equally has been the unsustainable security objective at many organizations.

A "best efforts" risk-based approach is more rational. Apply your best efforts to what is most valuable and what has the most impact on your business. In doing so, you prioritize levels of risk, which should be familiar ground to CIOs and other IT leaders from their work in business continuity and disaster recovery.

Determining what the organization's most precious assets are is hugely important but is often controversial. Some organizations believe that data is the most valuable asset needing protection. However, if risk attributes are assigned to an array of assets — data, software, networks, and personnel — it becomes evident that there is much more that needs consideration about penetration of and attacks on enterprise assets.

The notion of classifying business information assets to determine criticality is the least common factor in enterprise information security today, as shown by a recent survey by Info-

Deep Dive

World's sister publications *CIO* and *CSO* magazines, done with PwC.

This risk-based approach is not easy, and it requires a large mental shift for many organizations. But there's a good reason to make the effort: The bigger the stash of assets and the more complex the rules, the harder it is to protect them. A more focused and less complex approach could better balance the risk with the benefits and let you actually achieve your desired protection.

2. Protect key assets with multilayered defense systems

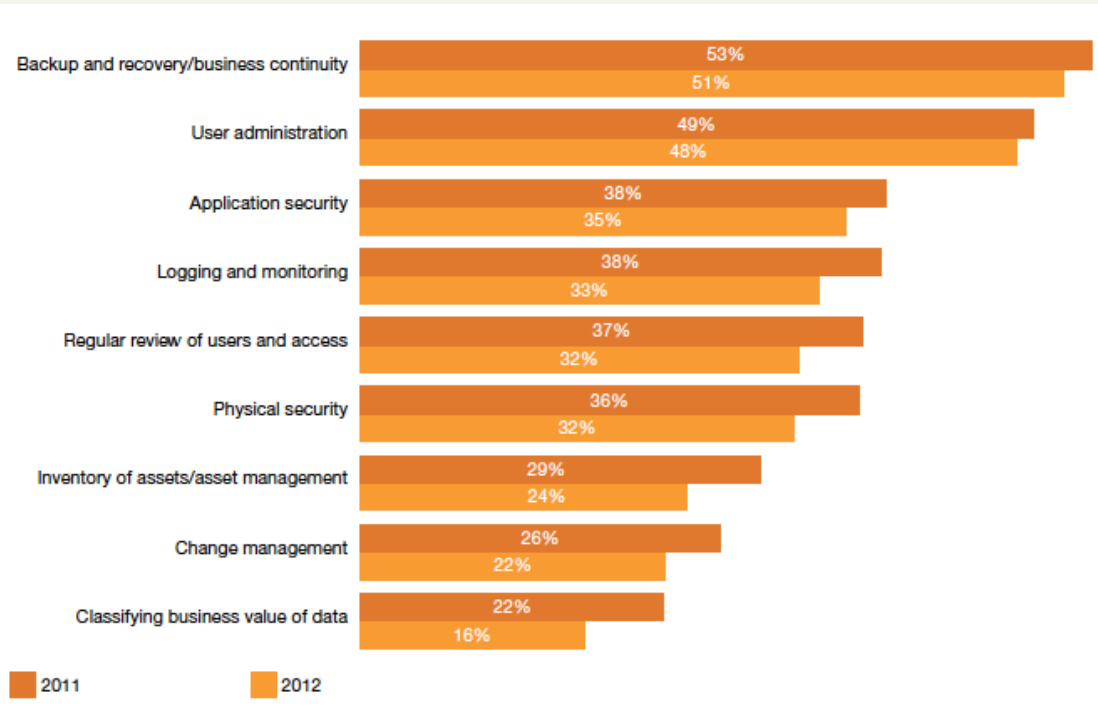
Any approach that requires 100 percent prevention is guaranteed to fail. There's no way to ensure that something is perfectly protected, so seek resilience rather than absolute prevention. Recognize that defenses have to be built from multiple components.

A better model for security is a biological one, where you can recover from and function despite infections or injuries. The biological system seeks to confine an intrusion to the system first infected so there's not a broader penetration. The biological system assumes there will be ever-evolving risks, and that one may be attacking now. All of these principles should be applied to the technologies and business practices you use to secure your business.

You should assume you're compromised, and develop a strategy around that assumption. (It's now clear that most companies are already compromised, whether by cyber criminals, competitors, or governments.) Understand that there are many sources of infection, not just the data center, PC, or mobile device.

Most biological systems also use redundancy.

There's no way to ensure that something is perfectly protected, so seek resilience rather than absolute prevention.



The elements included in enterprises' security policies. Value classification — the core of risk analysis — is sadly the least-common element. *Source: Global State of Information Security Survey 2013 by PwC, CIO magazine, and CSO magazine*

Deep Dive

Do the same for your security approaches. Intel CIO Kim Stevenson has described a three-tier approach that her company has effectively used that is based on this principle.

A tiered approach to access makes sense, using read-only or otherwise tiered containers — the equivalent of keeping your precious jewels in a safe in the house or locking your car even in the garage. You should couple such an approach with basic protection against accidents, such as requiring encryption and password sign-in to gain access to information in the first place — the equivalent of locking the house door and setting the alarm before you leave.

Deal with vulnerabilities in the design rather than after the fact.

Multilayered defense systems for software rely heavily on a combination of human scans and scans by software designed to identify vulnerabilities. You embed security into the software development life cycle with techniques such as risk analysis and peer review of code (sometimes by a QA organization), and you use commercial software that can check for vulnerabilities. There is currently no single software package that can scan for all potential vulnerabilities, so combine manual reviews with multiple scans by different threat identification packages. "Deal with vulnerabilities in the design rather than after the fact," says former Visa security exec Totev.

A good resource for understanding what to look for is the Open Web Application Security Project (OWASP), a nonprofit organization that provides insight into vulnerabilities and suggests mitigations.

A critical layer is identity management. Several technologies are available to do that, with differing hurdles for users and systems to jump. How many identity checkpoints you impose should relate directly to your risk analysis, and of course you should also use isolation to limit a compromise's reach. Biological systems typically do both.

An example of the combination of identity-based authentication and isolation is Salesforce.com. It uses two-factor authentication twice to allow access to its production environments, where the damage from an intrusion could be very high: A user must satisfy two-factor authentication to get into a trusted environment, and then satisfy a different two-factor authentication to get into an operational environment that is delivered through a dumb terminal from which no data can be moved or copied. A different standard is applied to email access, where the risk profile is different.

Identity management would be more effective if it could be applied to the data itself. DRM (digital rights management) at the information level would take such technology to a new level of assurance — but only if it could be deployed in a standard way, along the lines InfoWorld has suggested in its InfoTrust proposal. Reliable identification matched with consistent and portable permissions would reduce inappropriate access to information, even if devices and networks are breached.

3. Engage the people who use information to protect the assets they work with, both critical and noncritical

Until machines totally take over the universe, people are really the ultimate source of threats, and frequently the entry point for vulnerabilities. They're also a source of prevention.

Some of the most sophisticated threats arise through social engineering, where the bad guys worm their way in through social media and email contacts with unsuspecting users — particularly targeting executives and key operational staff. From there, deliberately and stealthily, the bad guys can assess the enterprise security provisions in place, and work around them. Put yourself in the shoes and mindset of both the bad guys and your own staff and business partners.

Because people are often the conduit for the intrusion, include them in the prevention. Stop automating them out of the process, as has been the standard IT mode for the past two decades. The "loose lips sink ships" management style from the pre-PC era was effective, making security everyone's responsibility, not something that employees could slough onto someone else. Today, it again needs to be a core component of modern information security. Not only will it

Deep Dive

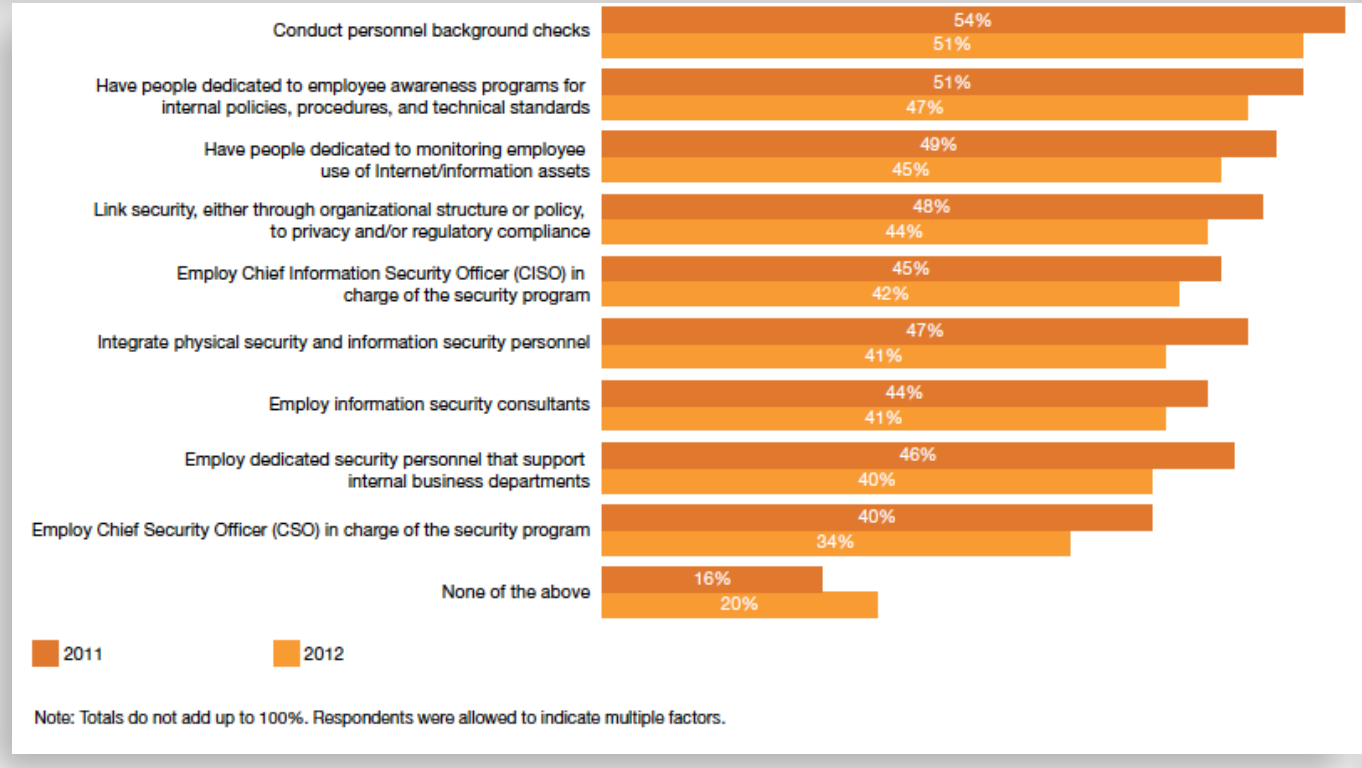
help those individuals avoid risky behavior, but there will be lots more eyes to observe whether something may be amiss.

When you bring people back into the security equation, don't neglect workforce and partner training and awareness. Yes, people can learn and apply what they're taught. That was the case at Long Island University, which several years ago began a security awareness initiative coincident with a shift away from PCs to iPads, mobile apps, and cloud services. The university is subject to HIPAA (Health Insurance Portability and Accountabillity Act) and FRCP (Federal Rules of Civil Procedure) regulations due to its medical school and status as a federal loan dispenser, yet found it could straightforwardly handle such regulations, CIO George Baroudi has reported. What differed was how IT engaged with the students and faculty, as a compliance-aware participant in the process, not an "in the basement" developer of technological constraints, he told *Information Week*.

Some industries have figured out how to make employees active participants in achieving key behaviors.

Some industries have figured out how to make employees active participants in achieving key behaviors. People are natural gamers, and creating game incentives for employees to avoid or detect threats can be a powerful antidote. Taking a quality-improvement management approach, some firms have used gamification techniques such as publicizing the number of incident-free days, creating both awareness and active participation in favor of safer behavior. Happily, if employees are screened, trained, and monitored to be trustworthy, the risk around the other, known-to-be-lower-risk information becomes even lower.

The good news is that a significant percentage of companies have many people-



Information security safeguards in place related to people. *Source: Global State of Information Security Survey 2013 by PwC, CIO magazine, and CSO magazine*

Deep Dive

oriented security methods in place, as the *CIO/CSO*/PwC survey shows, even if not necessarily handled in a holistic, pan-enterprise way. However, that big-picture approach is critical to success, because only then can you architect and deploy a system that works.

4. Team with business partners to boost their (and your) immune systems

You now live in a big digital information and process world that encompasses the enterprise sources of raw material, production, distribution, after-sale service, and support. This is true whether you are in a business that produces tangibles (such as cars and electronics products) or services (such as schools and hospitals).

There's no way to build a wall around the modern digital ecosystem.

In the last decade or so, companies have become highly virtualized thanks to outsourcing (to providers, contractors, and cloud services), distributed workforces (also a mix of staff and contract), distributed workplaces (satellite and home-based offices), outsourced workplaces (such as call centers), and work-anywhere/digital-nomad workers.

There's no way to build a wall around this modern digital ecosystem. You see this futility in the loss of effectiveness of traditional defenses, such as passwords, virus protection, intrusion detection, and other signature-based detection methods. Threats change too dynamically, and indeed can now self-adapt. Sophisticated bad guys go directly to servers or networks and bypass user devices' password protections. Recent massive customer data thefts at major retailers and the revelations by former NSA contractor Edward Snowden should make this situation evident to all. While many companies fret over whether iCloud or Google Drive is a threat, their core systems are already deeply compromised more directly.

The notions of inside and outside the company rarely apply so cleanly any more. As a consequence, a top issue for CIOs is cascading risk. Customers may trust the enterprise with which they interface, but can that trust extend to every other entity that may be part of the supply chain?

You should work with your suppliers and other business partners to apply the concepts described in this article to all your systems, not just the ones that interact. After all, there are likely more connections to exploit than anyone realizes, and having a common security framework is more likely to work than having multiple frameworks in place. (Of course, the implementation will need to vary based on the core risk analysis for each entity.)

Sharing best practices is synergistic. And active partnering is a far better approach than merely using contractual threats.

You can expect more demands from your customers, regulators, investors and others to demonstrate your security prowess and perhaps to demand to independently test those defenses. As part of this assurance, a "statement of applicability" will be requested, wherein the specifics must be provided of how broadly security measures are applied. This ties into the "you can't protect everything equally" points we've already raised. The costs of security are rising. Although they are an inevitable part of doing business, the costs can be managed at reasonable levels if you focus on the things that truly matter.

Some companies take a "checklist security" approach where they can enumerate the tactics they've followed to explain away the inevitable information losses to regulators and customers. They knowingly implement this checklist approach not because it works but because it minimizes the risk of lawsuits or fines. The checklist approach is an indictment of the status quo — a strategy that tacitly acknowledges the current perimeter approach is failing but doesn't offer a better alternative. The checklist pretense is no longer adequate.

5. Make security a business problem — not just IT's problem

Information security isn't just an IT or technology problem — it's fundamentally a management problem that few organizations treat as such.

Yes, the enterprise will look to the CIO and

Deep Dive

CISO for leadership on information security, but accountability has to be more broadly shared. Technology and security organizations can't be held accountable if the actions of individuals outside IT are the basis for compromises.

It's time to think of this evolving information security model as holistic security, using multiple technology and management techniques, with broad buy-in and accountability, layered and tailored to the estimated risk and value.

Broad governance is key, requiring actions and responsibilities across the entire organization, engaging employees, customers, suppliers, the C-suite, and the board as active participants. It requires management to assess, actively manage, and hold accountable managers, employees, and business partners — not deflect responsibility as a technology failure by the IT or security organization.

Broad governance is key, requiring actions and responsibilities across the entire organization, engaging employees, customers, suppliers, the C-suite, and the board as active participants.

For example, is Marketing using CIO-approved cloud or business analytics providers, which have demonstrated security capabilities? Do suppliers who routinely access critical data use compliant security processes? Does the board communicate through protected channels or does it distribute financial and sales data as attachments via open-environment emails? (Emails are never secure, and legal disclaimers at the end of the message are a false palliative.)

You need a pan-enterprise security governance similar to how HR or Legal operate in leading companies, with engagement from the board of directors down to the individual employees. Notice the phrase "operate in leading companies" — that's key, because too many companies confuse lots of rules and procedures with effective governance. If you tie up your staff in knots in the name of security, you won't gain security and, in fact, you are likely to be less secure, as people struggle to comply or, worse, stop trying and instead actively work around the barriers you've created.

Effective governance means enabling and encouraging people to do the right thing as the path of least resistance wherever possible. Monitor their performance, educate and retrain them when necessary, and apply both incentives and penalties for a pattern of noncompliance.

For example, if you have many employees who work in the field or at home, provide a secured cloud storage option that works with popular devices, so they're not tempted to use their own or, worse, resort to thumb drives, recordable CDs, and personal emails to maintain access to data when not at their desk. Do some internal phishing to identify employees who need further training or perhaps impose penalties such as loss of bonus or even loss of position for repeat or egregious lapses. Reward individuals and business units that are proactive in their safe practices and that act on suspicious behaviors.

Getting a flu shot does not assure you won't catch the flu, but it is a powerful tool that works best when combined with good hygiene and other defenses. Some enterprises perform self-assessments or routinely hire ethical hackers. Various industry groups have assessments you can do yourself or hire a professional to do. Use them. Government agencies such as the FBI also can help.

Monitoring and pattern analysis technologies, such as DLP (data loss prevention), database logging, security event tracking, and information-forensics tools, can help, too. They're not that useful as a preventive real-time shield, but they can deliver the benefit you really need: identifying data theft, fingerprinting it, and gaining the very useful understanding of how data is moving, who's doing what with it, and when it's trying to leave your systems.

The digital age came faster than security pros could adapt

It's true that the efforts to digitize business over the past two decades have occurred swiftly and often not so obviously until a tipping point was reached. So it's understandable that the information security model hasn't evolved as quickly as the environment you operate in.

But it's now clear that the mismatch is huge, and the only reasonable way forward is to adapt to the new ecosystem: Change your focus to risks and people.

It's time to stop trying to protect information in the network-connected era the same way

Deep Dive

you did in the "only in the data center" era. The perimeter approach is equivalent to the Middle Ages philosophy of protecting cities with fortress walls when the enemy has air superiority.

Of course you can and should put a perimeter defense around the most critical cores. Access control is the best defense, because the fewer people and devices that can access what is truly critical, the less intrinsic risk you have. If you grant access, you must trust those who have the access, because a determined person will find a way around your defenses.

Your focus should increasingly center on holistic risks and factoring people more prominently in your IT security approaches. Information security is not a set-and-forget policy or technology exercise. Risks change, the nature of information changes, as do the business contexts, business relationships, and operational contexts. People will always game around obstacles. Having an organization where information security awareness and responsibility belongs to everyone increases the chances that the unknowns will be identified faster.

Your focus should increasingly center on holistic risks and factoring people more prominently in your IT security approaches.

Companies have to accept that losses and breaches will occur, and thus change the mindset from absolute prevention to targeted prevention combined with resiliency and a notion of acceptable loss — the approach common to biological and human systems.

For 40 years, security efforts have focused on the equipment and, to a lesser extent, the data — removing the human factor in an attempt to reduce surprise and behavioral variations. That was a mistake. Your key vulnerability and key line of defense are one and the same — people. Security is ultimately a human responsibility shared by everyone — it's not an IT problem alone. Security-minded management must be made standard across the enterprise, where accountability is real and awareness is high: that proven "loose lips sink ships" approach that defense security experts generally call a counter-intelligence model.

We don't mean to suggest this shift is easy or swift. But it is necessary. ■

Bud Mathaisel *is a former global CIO at Disney, Ford, Solectron, and Achievo who now does research, writing, and consulting on information technologies. He also serves on the board and audit committee of E2Open and on a special advisory board for Honda Finance, North America.*

Terry Retter *spent 14 years as a director at PwC's Center for Technology and Innovation. Prior to that, he had been a senior IT leader at DHL and CIO at other companies. Currently, Retter coaches businesses in the effective use of Internet and social media marketing, based on his eight years of running an online retail store.*

Galen Gruman *is an executive editor at InfoWorld who focuses on consumerization of IT and mobile technology.*