The Rise of User-driven IT: Re-calibrating Information Security for Choice Computing

Recommendations from Global 1000 Executives

Report based on discussions with the "Security for Business Innovation Council"

1. Anish Bhimani, Chief Information Risk Officer, JP Morgan Chase
2. Bill Boni, Corporate Information Security Officer (CISO), VP Enterprise Information Security, T-Mobile USA
3. Roland Cloutier, Vice President, Chief Security Officer, Automatic Data Processing, Inc
4. Dave Cullinane, Chief Information Security Officer and Vice President, eBay
5. Professor Paul Dorey, Founder and Director, CSO Confidential and Former Chief Information Security Officer, BP
6. Renee Guttmann, Vice President, Information Security and Privacy Officer, Time Warner Inc.
7. David Kent, Vice President, Global Risk and Business Resources, Genzyme
8. Dave Martin, Chief Security Officer, EMC Corporation
9. Dr. Claudia Natanson, Chief Information Security Officer, Diageo
10. Vishal Salvi, Chief Information Security Officer and Senior Vice President, HDFC Bank Limited
11. Craig Shumard, Chief Information Security Officer, CIGNA Corporation
12. Denise Wood, Chief Information Security Officer and Corporate Vice President, FedEx Corporation

An industry initiative sponsored by RSA, the Security Division of EMC

The Security for Business Innovation Initiative

Business innovation has reached the top of the agenda at most enterprises, as the C-suite strives to harness the power of globalization and technology to create new value and efficiencies.

Yet there is still a missing link. Though business innovation is powered by information; protecting information is typically not considered strategic; even as enterprises face mounting regulatory pressures and escalating threats. In fact, information security is often an afterthought, tacked on at the end of a project or – even worse – not addressed at all. But without the right security strategy, business innovation could easily be stifled or put the organization at great risk.

At RSA, The Security Division of EMC, we believe that if security teams are true partners in the business innovation process, they can help their organizations achieve unprecedented results. The time is ripe for a new approach; security must graduate from a technical specialty to a business strategy. While most security teams have recognized the need to better align security with business, many still struggle to translate this understanding into concrete plans of action. They know where they need to go, but are unsure how to get there. This is why RSA is working with some of the top security leaders in the world to drive an industry conversation to identify a way forward.

RSA has convened a group of highly successful security executives from Global 1000 enterprises in a variety of industries which we call the "Security for Business Innovation Council." We are conducting a series of in-depth interviews with the Council, publishing their ideas in a series of reports and sponsoring independent research that explores this topic. RSA invites you to join the conversation. Go to www.rsa.com/securityforinnovation/ to view the reports or access the research. Provide comments on the reports and contribute your own ideas. Together we can accelerate this critical industry transformation.

Business Innovation Defined

Enterprise strategies to enter new markets; launch new products or services; create new business models; establish new channels or partnerships; or achieve operational transformation.

Table of Contents

Introduction

An unstoppable force is knocking at the doors of enterprise Information Technology (IT) departments worldwide. Users are demanding a voice; and attempting to wrest away control. The traditional model whereby IT dictates all of the technology used in the enterprise is quickly crumbling.

With years, even decades, of PC and Internet experience now under their belts, most users today are no longer satisfied being passive recipients of technology. Computing is now central to their lives; not just something they do at the office. They want to choose the technologies that will make them most productive and bring them into the enterprise.

Some call it consumerization. While it's true the rapid adoption of consumer technologies – everything from smartphones to social media – is powering this transformation; it's more than that. Something else is going on. It's not just the IT department determining how consumer technologies will be used in the enterprise. The users are taking the reins.

User-driven IT has the potential to deliver huge benefits to users and their organizations. The enterprises which figure out how to unleash the power of user know-how and consumer technologies while managing the risks will win this high stakes game. Information security teams could be the most valuable players.

Security for Business Innovation Report Series

The Time is Now: Making Information Security Strategic to Business Innovation
Recommendations from Global 1000 Executives

Mastering the Risk/Reward Equation: Optimizing Information Risks While Maximizing Business Innovation Rewards
Recommendations from Global 1000 Executives

Driving Fast and Forward: Managing Information Security for Strategic Advantage in a Tough Economy
Recommendations from Global 1000 Executives

Charting the Path: Enabling the "Hyper-Extended" Enterprise in the Face of Unprecedented Risk
Recommendations from Global 1000 Executives

Bridging the CISO-CEO Divide
Recommendations from Global 1000 Executives

www.rsa.com/securityforinnovation

Over the past few years, information security has been shifting from a technical specialty to a business imperative. The challenges posed by user-driven IT are, like never before, testing the new skills that information security teams have been building. Making the transition to user-driven IT requires the ability to expertly manage risks to enable business innovation – all at accelerated speeds. Being out in front of these trends is critical for information security professionals; it could mean the difference between being strategic or irrelevant.

This sixth report in the "Security for Business Innovation" series looks at how user-driven IT is forcing information security professionals to recalibrate their approach to align with a rapidly changing environment. The guidance in this report was derived from conversations with a group of top information security leaders from the Global 1000 – the "Security for Business Innovation Council." The report lays out a roadmap for protecting information in a way that provides more choice for users while delivering business value for the enterprise.

"There's a head-on collision coming between our personal and professional lives, and it is consumer technology that is going to cause it. Information security needs to be the advocate for a more engineered journey into this integrated place that we're going to, where our personal and professional lives converge."

Denise Wood
Chief Information Security Officer and Corporate Vice President
FedEx Corporation

"The pressure was building even pre-iPhone. If users didn't have a corporate portable computing device, they started buying their own and wanting to connect it to the enterprise. Now it's exploding because there are so many different platforms, the prices are coming down and their friends have shown them how great it is to have one."

Dave Martin
Chief Security Officer
EMC Corporation

"IT security teams will never be able to stop the pace – technology is on a roll. Every one of the conversations we've had about security not being a business barrier but rather an enabler –– if anyone still thought they were theoretical – have to move from theory right into practice now."

Dr. Claudia Natanson
Chief Information Security Officer
Diageo

User Demands

Today's users know what works for them. In some cases, they are way ahead of the IT department; especially in understanding how to leverage consumer technologies for their particular jobs. Admittedly, some of their fascination with the latest technology is the "coolness" factor. But enterprises that dismiss users' demands as frivolous do so at their peril. There are real business benefits to be had. Ultimately, users want to use the same powerful productivity tools that help them lead their personal lives to conduct business.

To date enterprises have not exactly been ignoring consumer technologies. Over the years, enterprises have enabled the use of mobile phones and e-mail devices (albeit mostly company-issued) and have used social networking for narrow applications such as HR recruiting, PR campaigns and internal collaboration among employees. But users want more – more choice in computing platforms, increased use of smarter mobile devices and better access to social networking sites.

The draw of the mobile social web

Probably the biggest factor in ramping up user demands has been the recent extraordinary growth of the mobile social web. Enterprise employees come across examples from the consumer world every day that make them ask, "Why can't we use this technology for work?"

For example, they pay their bills while they are traveling in the back of a cab thousands of miles from home. They check inventories and make arrangements for a car purchase through the salesperson's mobile device while standing on the car lot. With one click on their smartphone, they order a taxi, which meets them at the curb seconds later.

So it's no wonder they are asking questions like, "Why can't I use my own netbook instead of the antiquated PC I've got on my desk?," "Why can't I carry a thin tablet rather than schlep a fat laptop across the country?," "Why can't I find new customers as fast as I find new restaurants with the latest smartphone app?," and "Why can't I go to my favorite micro blogging site to get the latest buzz on our industry?" To top it all off, since computing devices and applications have become as individual as the clothes people wear and the cars they drive – users are also asking, "Why does IT have to tell users how to interact and communicate?"

The demands aren't just coming from the fresh-out-of-college new recruits or the marketing department; senior executives from every corporate department are beginning to make requests. For example, the CEO wants to move his whole C-level team from laptops to tablets so they can easily carry the device around with them to make timely decisions.

The sales force wants to access their customer relationship management (CRM) application while they are on the road from their smartphones. Executives want smartphone access to approve travel expenses and purchase orders.

Even "old school" bosses who used to think social media was just a time-suck are starting to come around. They are witnessing their tech-savvy employees in action. Scenarios like this one are playing out: Executives sit around the boardroom table coordinating a market research study to determine what features to add to their new product; meanwhile employees use their personal smartphones to text and tweet their way to some possible answers before the meeting is over.

The potential payoff of user-driven IT is huge. Choice computing would enable users to choose the computing platforms and applications best-suited to them; thereby fueling productivity. If users supply their own corporate/personal machines, the cost savings could be significant. Increased use of mobile devices like smartphones, tablets, or netbooks could create tremendous efficiencies. Increased access to applications – from the latest micro blogging site to the latest smartphone app – has the potential to cut time-to-market; provide real-time market data for faster decisions; and even generate revenue.

Of course the potential risks – including legal issues, data leaks, privacy breaches, malware explosions – are also substantial. But smart information security teams will not stand in the way of progress; instead they will listen to user demands to figure out a strategy that balances the risks and rewards. And they'll act fast. Because the longer it takes, the more likely it is that users will simply go around information security and do what they want anyway, violating the security policy and exposing organizations to risk.

"These personal productivity and collaboration tools are just so easy to use and so powerful that everybody's got to have one. We're trying to understand: what happens when you want to leverage these powerful, consumer platforms for unbridled collaboration at work?"

Denise Wood
Chief Information Security Officer and
Corporate Vice President
FedEx Corporation

"Smartphones are here to stay and they are proliferating. When employees are given the choice to upgrade their corporate handset by making an additional investment, most of them upgrade to a smartphone."

Vishal Salvi
Chief Information Security Officer and
Senior Vice President
HDFC Bank Limited

"You've got to treat users as grownups. The nanny state of IT can't continue – where the attitude is, 'IT end-users cannot be trusted, we will therefore make the decisions for them.' You cannot expect to manage end-users that way anymore. Control is largely gone, you may not like it, but you're stuck with it. So make sure that users understand their responsibilities and enable them to be grownups."

Professor Paul Dorey
Founder and Director, CSO Confidential and
Former Chief Information Security Officer
BP

The Timeline

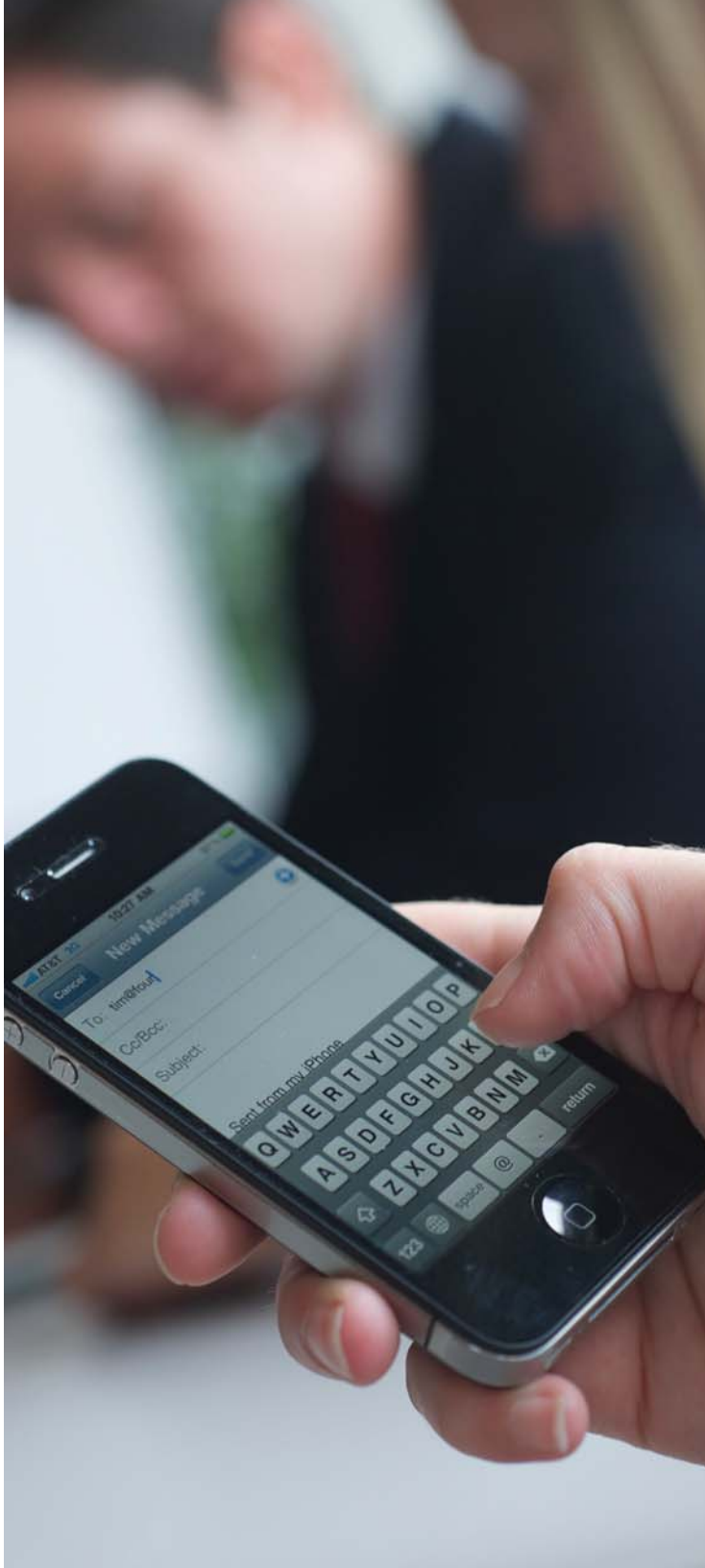
The exact trajectory for user-driven IT is anybody's guess. But the general consensus of Council members is that the use of consumer technologies in the enterprise will ramp quickly as demand swells and the business case gains credence. Also, the availability of new virtualization technologies now makes the roll-out of consumer devices and applications more feasible. Therefore, information security teams need to start planning now.

To keep up with rising user demand, the ongoing risk assessment and management process must be designed to operate at top speeds. The world of consumer technology operates at a much different pace than traditional enterprise technology. Product lifecycles are extremely fast. And as consumers, users are accustomed to instant gratification. Users will continue to make new requests as new mobile devices and social media applications are constantly introduced. Enterprises will also want to take business advantage of the new technologies as quickly as possible.

The invasion of consumer devices

Recent research provides some indication of just how fast consumer technologies may invade the enterprise. For example, the adoption rate for new mobile devices could be dramatic. In a recent survey, half of all respondents (IT professionals) said that at least 60 percent of employees at their companies will be smartphone-equipped in the next 24 months. And the bulk of these newly-connected devices – perhaps as much as 80 percent – will be employee owned.[1]

Choice computing is becoming more popular as enterprises are motivated by the potential for decreased costs. Studies show that well-managed employee-owned notebook programs can deliver significant savings. According to Gartner, "Compared with less-managed deployment scenarios, a managed virtual machine on an employee-owned notebook offers total cost of ownership (TCO) savings of between 9 percent and 40 percent when compared with company provided notebooks."[2] In certain geographies such as India, there may be less incentive to move to employee-owned devices. This is because enterprises often rent PCs from a service provider, which configures and maintains the machines. Under this model, computers are already an operational rather than capital expenditure. But elsewhere, many organizations are recognizing the benefits of moving to employee-owned devices. For example, Kraft Foods, the second largest food company in the world, recently announced a "bring your own computer (BYOC)" program for employees with the intention of decreasing costs and increasing flexibility.[3]



Increased revenue could also drive adoption of consumer technologies in the enterprise. For example, innovative new enterprise applications – either off-the-shelf or custom-designed – could become powerful sales tools. Manufacturers might increase retail coverage by arming their sales teams with new mobile apps; or services firms could increase the value of customer engagements with powerful smartphone apps for their consultants. The incentive for investing in enterprise applications will increase as there are more consumer success stories – like the new eBay app for the iPhone® device which went live in August 2009 and rapidly generated more than $600M in 2009[4] revenue in just 4 months.

Studies suggest that new Internet-enabled mobile devices may rival the PC as the chief computing platform in the enterprise. A survey of mobile employees found that 63 percent prefer a smartphone over a laptop as their primary mobile device.[5] Smartphones are set to outpace sales of desktop computers by 2012; with sales of smartphones predicted to more than triple to over 491 million units.[6] And according to analyst firm IDC, "the number of mobile devices accessing the Internet will surpass the one billion mark over the next four years."[7] This doesn't mean the death of the PC is looming, but for some users, its days are numbered.

The inevitable shift towards social media

Most information security leaders accept that broader use of social media in the enterprise is a matter of "when" not "if." However at the moment, many enterprises still do not provide users with completely unfettered access to social media. A common concern, which has nothing to do with security but is a human resource management issue, is that workers will spend too much time on social sites and productivity will suffer. Many companies are opting for selective access based on perceived business benefits.

But the reality is that the sheer volume of people on social networking sites makes them a powerful communication channel that may

be hard for enterprises to resist. After triple digit growth throughout 2009, Facebook is poised to hit the 500 million subscriber milestone in June, 2010.[8] Twitter is at 105 million[9] and LinkedIn at 65 million subscribers globally.[10] Besides having vast numbers of subscribers, social media sites now control more online traffic. A recent study by Network Box looked at 13 billion URLs used by businesses and discovered that in the first quarter of 2010, 6.8 percent of all business Internet traffic goes to Facebook.[11] This means that employees are visiting Facebook from the workplace more than any other internet site, including Google. This is happening in a world where many enterprises still block or at least restrict access to social networking sites. And a study in late 2009 found that 57 percent of U.S. employees who do have access to social media *are* using it for business purposes.[12]

Most enterprises plan to increase their use of social media in 2010[13]: 72 percent of companies plan to invest more in recruiting through social networks; and 79 percent of the largest fortune 500 firms plan to use Twitter, Facebook, YouTube or corporate blogs to communicate more with customers and other stakeholders. Social media is quickly becoming the dominant channel for branding campaigns. For example, through its "Keep It Coolatta Sweepstakes," Dunkin' Donuts has attracted over 800,000 "fans of the brand." American Express OPEN's "Open Forum" has increased unique visitors by 525 percent in a year to nearly 1 million.[14]

Beyond marketing applications, analysts predict that we'll start to see social media used as a general communications tool. For example, Gartner estimates that, "By 2014, social networking services will replace e-mail as the primary vehicle for interpersonal communications for 20 percent of business users."[15] As Gen-Y young adults make up more of the workforce, they will not accept the limitations of email and will expect their business communications to have the same functionality as social media. Workforce demographics have the potential to bring a tidal wave of change.

Consider that after Gen-Y, the first wave of Millenials (born around 2000) will enter the workforce. Millenials have only ever known social media and smartphones. It's how they interact with each other and the world.

So are enterprises starting to plan for the inevitable onslaught of consumer technologies? It is still early in the game, but some Council members estimate that currently about 25–30 percent of enterprises have already started integrating specific plans for user-driven IT into their IT strategy, including enabling more choice and access to mobile and social computing. Enterprises that don't include it in their IT strategy may begin to see "shadow IT;" as users will buy consumer devices, applications and/or services on their own and start using them for enterprise business. A better approach is to plan for it now so as these trends gain momentum, information security teams are ready to manage the risks.

> "The demand keeps building and building. Meanwhile information security is doing research trying to figure out the requirements. You have to able to keep up. You have to know what's coming next year so you can figure out what to put in place now."
>
> Dave Cullinane
> Chief Information Security Officer and
> Vice President, eBay

“If new consumer devices are rolled out as company-provided equipment, it requires additional investment, so growth could be slow. But for companies that can perfect allowing people to use their own consumer devices securely, the adoption rate will be faster.”

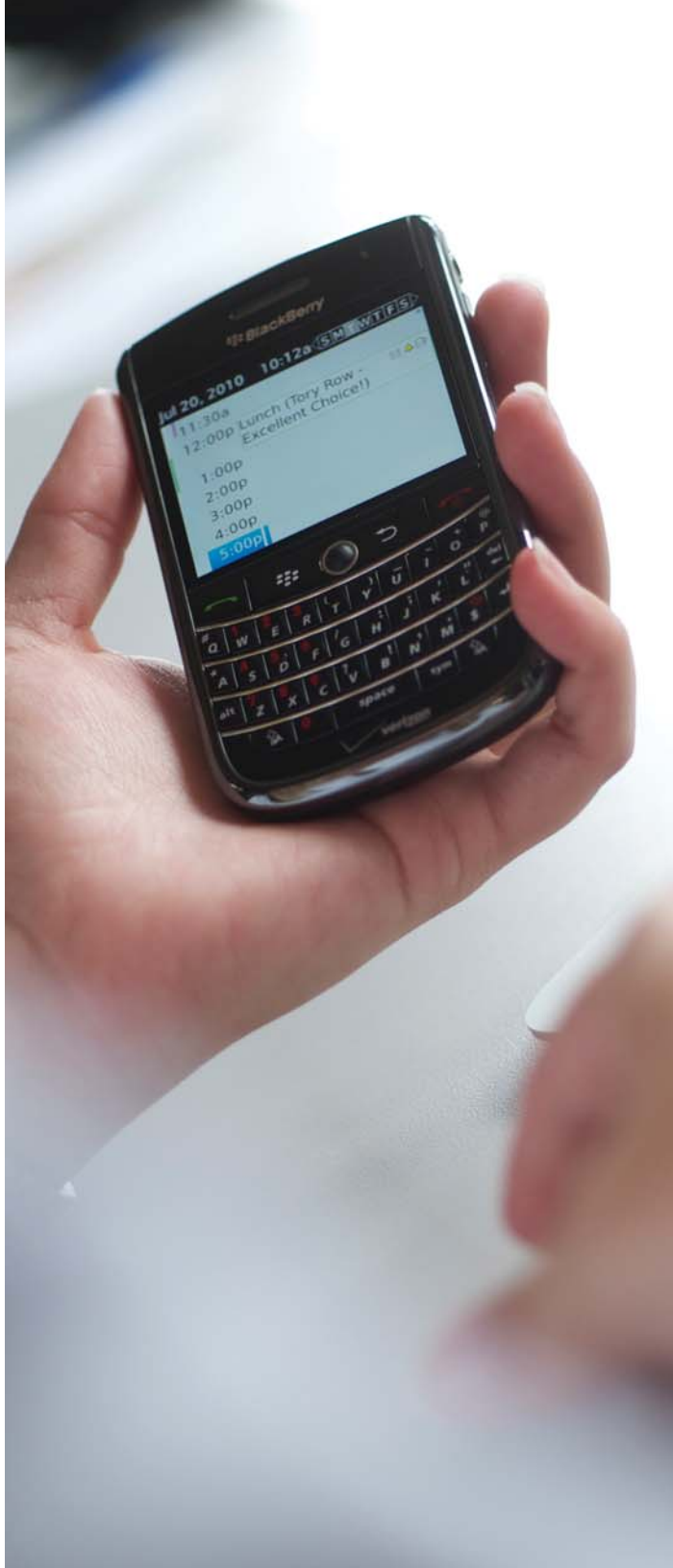
Dave Martin
Chief Security Officer
EMC Corporation

“Adoption of social networking is going to be completely driven based on the business case and how does it add value to the business? So far none of the business guys have come to me saying, ‘I need access because it will increase my revenue.’ But the day that starts happening, as soon as there is a need, we will have to have a solution. It’s not something the CISOs or any security teams are going to control. It will be business driven. CISOs and security teams need to be agile to these changing business dynamics.”

Vishal Salvi
Chief Information Security Officer and
Senior Vice President
HDFC Bank Limited

"I think in the past 12 months, the recession has limited a lot of investment spending on new technology so enterprise use of consumer technology is lagging, and as an industry we're still at the innovator or early adopter stages when it comes to security. But a tidal wave of change is about to erupt over a three-year timeframe, when enterprises in every industry are going to see significant impact. And over the next three years, we're going to find a lot of land mines."

Bill Boni
Corporate Information Security Officer (CISO),
VP Enterprise Information Security
T-Mobile USA



Even if users are clamoring for more, enterprises are not just going to open the gates and let everything in. The adoption of consumer technologies in a particular enterprise will be affected by many factors, such as the company's culture, user population, industry, geography, business climate, existing infrastructure, threat landscape, regulatory environment – and ultimately the company's appetite for risk.

The key is not to be in denial. User-driven IT is real – start figuring it out now. Don't let the users control the plan by going around security to bring in restricted devices and access unauthorized applications. As users take the driver's seat, information security must navigate – allowing users to choose their own types of cars; but explaining what roads are safe to drive on, providing safety requirements for their vehicles, educating them on safety procedures, and putting up guardrails so they don't go over a cliff. The following six steps provide a roadmap for information security teams that will position them to give users more choice in computing – partnering with key players across the organization to proactively weigh the business benefits against the risks and determine the right implementation strategy.

"It is very difficult for organizations to 'carte blanche' just say, 'Okay, we're just going to give everybody access and open up our boundaries to allow the use of any device.' Because the enterprise still has the responsibility for the protection of its data. So even with the best intentions we have to guardedly introduce things so that we're managing the risk as we roll it out."

Dr. Claudia Natanson
Chief Information Security Officer
Diageo

1. Shift Minds to the Times

Enabling user-driven IT requires a shift in information security thinking. This shift has actually been in the works for several years. Ideas like aligning to the business, taking a risk-based approach and moving to a data-centric model are nothing new. Now they are just more urgent. The rapid adoption of consumer technologies, compounded with other mega trends like cloud computing, is forcing information security teams onto an even steeper learning curve.

First and foremost, information security professionals (and their counterparts in IT) will have to get comfortable with relinquishing control. Your role becomes less about control and more about oversight. Understand what the business is trying to do and then help manage the risks. The traditional model where IT and security dictate everything to users is now changing. Increasingly users will actually be making decisions about how technology is used in the enterprise.

De-perimeterization has been discussed in security circles for years. User-driven IT further erodes the notion of protecting the perimeter and demands laser-like focus on data and applications. Also recognize that certain basic assumptions about information security no longer apply. For example, the concept of controlling the end-point and not allowing personal assets to connect to corporate systems has been a standard pillar of the security model for years. But in the age of user-driven IT, these assumptions are no longer valid.

"Information security has to be completely plugged into the organization's business and direction. You have to understand the pain, gaps and challenges; so whenever a new technology arises, you'll have the ability to balance the "control instinct" with an informed understanding of the benefit and needs."

Bill Boni
Corporate Information Security Officer,
VP Enterprise Information Security
T-Mobile USA

This shift in thinking also calls for a re-evaluation of what is important to protect; you simply won't be able to protect everything. Work with the business to identify the organization's true "information crown jewels." For example there may be a level of protection applied to certain types of data that is simply not necessary, such as day-to-day e-mail and general office content (depending on legal and regulatory obligations). Based on an understanding of the business processes, information security should also be questioning why certain data is even being collected or retained in the first place. If it doesn't need collecting or storing, it won't need protecting.

Shift your thinking from…	To…
Security specialist	Business risk consultant
Control	Oversight
Paternalistic relationship with users	Partnership with users
Perimeter defense	Data and applications protection
End-point is a PC or laptop	End-point could be anything: smartphone, tablet, netbook, kiosk, home PC …
End-point is owned and controlled by the enterprise	End-point is not necessarily owned and controlled by the enterprise
Users don't know anything about technology	Users know a lot about consumer technologies and how to use them to be more productive
Protect everything	Focus on a more selective set of crown jewels

"For us as security people working in this new world, it's about, how do we relinquish control? Security and control historically have been linked together. If I know where my perimeter is – where my data is, the physical location of things, I feel confident. As a security person, it feels like you're flying blind, but one of the things that you have to get used to is losing control of your perimeters."

Dr. Claudia Natanson
Chief Information Security Officer
Diageo

"I think it's a situation where we've got to sit back and take another look at, what are really the crown jewels. What are really the things that you're trying to protect and why are you trying to protect them?"

Craig Shumard
Chief Information Security Officer
CIGNA

2. Reframe Users as Assets

The average person has become a sophisticated technology user; easily configuring devices, synchronizing data, downloading apps, spinning up websites and navigating social space. Although some users apply their skills in ways they shouldn't, like circumventing security controls (and a few may even be malicious), most are looking to work faster or serve customers better. Information security professionals who embrace user-driven IT will see user know-how as a potential asset and figure out how to leverage it for the enterprise and security team.

Listen carefully to what users want to do and determine which requests could translate into real business value; then focus on enabling them to realize that value. For example, if a sales person is able to find 60 customers a day on Facebook, it wouldn't make sense for the security team to shut down that access. Instead they should do everything in their power to enable it. If employees are willing to make themselves available 24/7 to help drive the business forward, don't make it tougher for them by asking them to carry two devices. Make it easier by supplying one device for personal and business use.

Tailor your approach to the various user groups; each will have different needs. For example, knowledge workers may increasingly want to use smartphones as their primary computing device so they can take advantage of all the mobile applications. But since many of their jobs require traditional document creation, they'll probably opt for a laptop as well. Other user groups such as call center workers have little need for smartphones; their needs could continue to be met with a standard desktop. Employees in sales and marketing may legitimately need access to social media to communicate with customers whereas those in the accounting department don't have the same pressing business need. User needs will undoubtedly change over time as ways of working and communicating evolve.

In the past, user education was a one-way street. Now it needs to be re-invented as a two-way conversation. You know about information security and users know about consumer technologies and how to use them to fuel productivity. Think of your user population as a powerful tech-savvy army that can educate you about the latest gadgets and applications.

"As technology matures, we'll have to ration out more access and platforms; while trying to keep everyone happy. So you might have a happy user who has access to everything and the performance they want, but we also need to make IT happy by maintaining reasonable cost of ownership and supportability and keep security happy by managing the risk during this whole process."

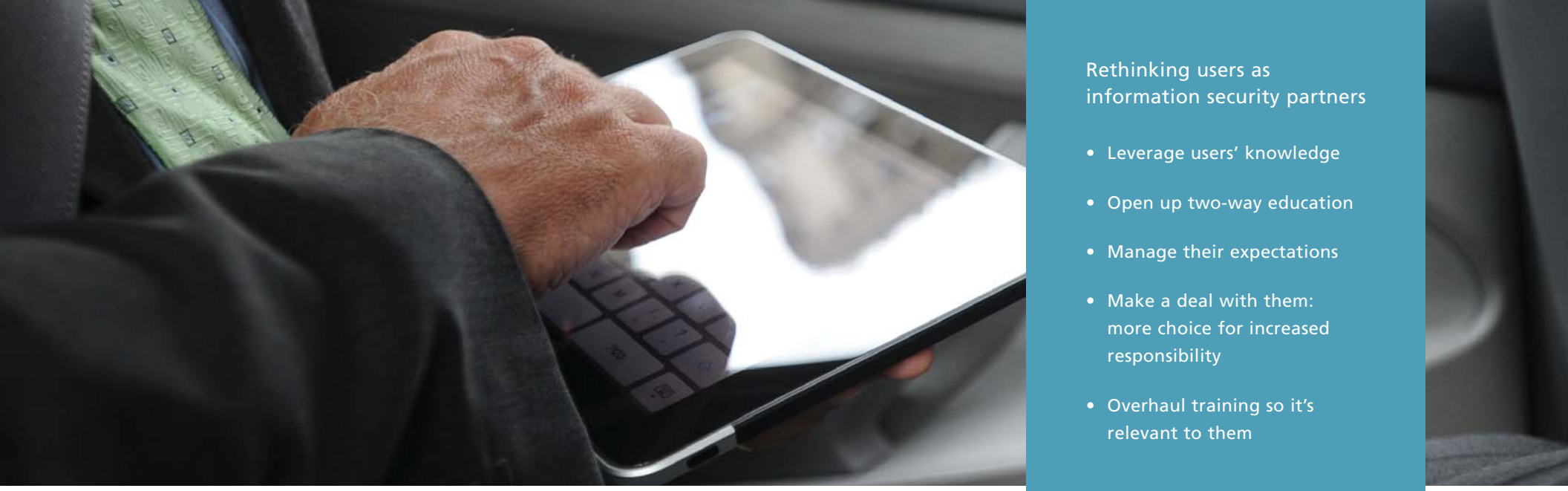
Dave Martin
Chief Security Officer
EMC Corporation

"One of the problems with training and awareness today is that often there isn't enough customization to reach specific groups. All too often training is packaged as a one-size-fits-all, but it's got to be packaged to target a specific constituency group in the way that they learn and operate. If it's done in a fashion that makes sense to them and is meaningful to them, it will have a much greater impact."

Craig Shumard
Chief Information Security Officer
CIGNA

"It's like needing both a belt and suspenders. Users need training – they need to be given the chance to do the right thing; and told what the right thing is. But then occasionally people forget or make a mistake, or there's someone who tries to circumvent things, so that's why you need other controls – to catch that when it happens."

David Kent
Vice President, Global Risk
and Business Resources
Genzyme



Rethinking users as information security partners

- Leverage users' knowledge
- Open up two-way education
- Manage their expectations
- Make a deal with them: more choice for increased responsibility
- Overhaul training so it's relevant to them

Consider setting up a process where users keep your team informed of new developments in consumer technologies. Set up an internal social networking platform to enable users to have collaborative discussions on new productivity tools and the corresponding business benefits and security issues.

Recognize that it's not an all or nothing proposition. Users may want everything now, but it can be a phased approach. The trickiest part will be to manage their expectations. Do this consciously and be transparent. Communicate why certain technologies are allowed and when others might be adopted. You won't be able to say "no" but perhaps "not yet and here's why." Be aware that just opening up the flood gates and counting on your ability to close them later if you need to is not a winning strategy. It's better to start with less and allow a little bit more at a time.

Make the tradeoffs clear: more choice means more responsibilities. For example, users will need to have a thorough understanding of the enterprise's information protection and acceptable use policies, and be accountable for upholding these policies. Also, the ability to use a particular device may be accompanied by specific requirements for that device's operating system, browser, apps and security features. Clear policies need to be established regarding who users should call if their devices break; users may have to take on responsibilities for arranging support services. Users must be ready and willing to understand the terms and conditions of enjoying more choice in computing.

Many Council members believe that enabling user-driven IT requires an overhaul of user training. Go beyond teaching security procedures and rules. The education process should provide a fundamental understanding of what information needs to be protected, how it needs to be protected and why protecting information is not only important to the company but also to users themselves. To be successful, user training should be customized to each user group, and reinforcement is essential. Although user training is crucial, all Council members stressed that you can't just rely on user training; it has to be balanced with other controls such as data leak prevention to ensure users don't unintentionally make mistakes or insiders aren't able to do something malicious.

3. Support Calculated Risk-Taking

As defined in a previous report, information risk management is "identifying and measuring the risks to information, and ensuring that the security controls implemented keep those risks at an acceptable level to protect and enable the business."[16] Therefore, to help keep the risks of user-driven IT to an acceptable level, you have to know the risks and your organization's risk appetite. Opening up access to computing platforms and social applications introduces a whole new set of risks that are compounded by escalating compliance and legal obligations and an evolving threat landscape.

Consumer technologies represent enormous opportunity, but there are still many uncertainties about the risks. Given the current environment, some enterprises will decide to increase their risk appetite to reap the potential rewards. Information security's role will be to truly understand the risks, carefully and thoroughly communicate them to the business, and help the business make informed risk/reward decisions.

The legal and compliance issues around user-driven IT will be some of the thorniest. Virtually every global enterprise has to protect the privacy of personal information, ensure the integrity of proprietary financial data and safeguard customer data such as credit card numbers. The information risk management strategy for user-driven IT has to meet these various legal and compliance requirements while simultaneously loosening up control. This is a tall order. And at this stage, there are still many questions.

Issues of ownership and representation

Allowing employees or contractors to use their own personal mobile devices for work creates some challenging issues around rights of ownership. Some legal questions will be: Who owns the company data when it's on a personal device? What are the legal responsibilities of the corporation and the user for maintaining the device? In the case of a breach, for the purposes of an investigation, would the user be forced to give up the device? In some cases, it may be necessary to have users sign legal agreements regarding ownership of a mobile device and the data on the device. Technology solutions like virtualization and thin computing may help with these issues since the corporate data would not be stored on the device.

When it comes to social networking, most general counsels shudder at the thought of workers out there representing the corporation. Imagine a scenario whereby a pharmaceutical company employee sets up a social media site to discuss a particular disease and ends up unwittingly doling out medical advice. Or a financial services employee starts a blog to discuss investments but goes over the line and ends up in a conflict of interest

"A big security fear with choice computing is: what if data gets on a device, the device gets stolen and the data's now in the open? But virtualization of the user environment makes a lot of the concerns a moot point. Through virtualization, users can do their work but not actually be touching the data."

Roland Cloutier
Vice President, Chief Security Officer
Automatic Data Processing, Inc.

"You worry about idea ownership; because social networking is inherently outside the management and governance structures that we use in our day-to-day work life. By definition, it gets you beyond a comfort zone. So then it comes down to, "Who owns the ideas?"

Denise Wood
Chief Information Security Officer and
Corporate Vice President
FedEx Corporation

situation. It is a slippery slope. An effort that begins with good intentions to exchange public or non-sensitive information could suddenly veer into information that has obligations around it. Doing business in the world of social media will require that users understand their responsibilities in upholding the company's legal obligations and operate under the company's code of conduct.

The e-discovery conundrum

E-discovery also presents some challenges. Typically when a company gets served with a subpoena for data, the courts ask for paper files and any electronic records associated with the matter. Now beside e-mail or instant messaging (IM), increasingly records could be contained in many other places such as Blackberry® servers or Twitter™ micro blogs. What if a forensic image of a disk is requested, but the device is owned by the employee? What if a court case involves a disputed transaction for which the communications took place on Facebook? If the data requested is on a social networking site, how will the corporation retrieve it? In general, if data is not on corporate servers but on user devices or social media sites, how does the enterprise meet standard record keeping requirements such as the need to retain data for a specified time period (like seven years)? As with the adoption of any new technology, enterprises will need to revamp their record-keeping policies and processes to include new types of records.

Then there are privacy issues. What privacy rights can an employee expect when using a personal device for work? A recent court case in New Jersey shows how privacy issues could play out. In a dispute between an employee and employer, the court ruled in favor of the employee's right to privacy. Certain emails were not allowed as evidence as they were considered private communications, even though they were stored on corporate servers.[17] This case involved personal data on company assets; what will happen when it's company data on personal assets? How will privacy be affected? The information security team will need to work closely with the legal team to think through all of the potential privacy issues.

The growth of mobile malware

Other risks that need to be carefully assessed include new forms of malware. So far, viruses on the PC platform far outweigh viruses on mobile phones, but that will likely change. As the number of smartphones grows, the devices get more capable and the information on them more valuable; they will become more attractive targets. Hackers are already working hard at cracking all types of devices. Blackberry®, iPhone®, Android™ devices – and the like – are all at risk. And some have already succeeded such as the 2009 Sexy Space botnet which was aimed at the Symbian mobile device operating system.[18]

The cyber criminals are taking the experience they've built within the PC and web world and applying it to this new mobile space. Security researchers believe it will take much less time for mobile phone viruses to become money-making operations than computer viruses did. Over the next year, they expect to see the, "industrialization of smartphone malware."[19]

As choice computing takes hold, many users may choose the Mac® computer. Until now, Mac® computers have been relatively immune to the onslaught of attacks targeting OS flaws. As the Mac® computer becomes increasingly popular in the enterprise, it may spur on the development of new malware; for example the OSX.Iservice Trojan that targeted Mac® computers in 2009.[20]

Social networks might also become more prone to malware attacks. As social networks encourage application development on their platforms to feed the insatiable appetite of users, cyber criminals are developing applications that target these generally trusting users, turning social networks into another vector for malware. Already 57 percent of users report they have been spammed (a rise of 70.6 percent from last year) and 36 percent reveal they have been sent malware via social networking sites (a rise of 69.8 percent from last year).[21]

Another growing concern is the so-called "were-laptop." Similar to a werewolf, user-

owned systems seem clean and healthy during the day but become malware-laden at night while they prowl the Internet from the user's home. When employees bring them back into work, the machines broadcast viruses across the enterprise.

While current signature-based anti-virus solutions have difficulties catching much of the current malware; next-generation anti-malware solutions are emerging that employ new techniques – such as behavior-based approaches that monitor the stream of system calls that the program issues to the operating system. Over the past several years, security researchers have also been leveraging their experience battling against malware designers to proactively create anti-malware innovations that will help protect information on new computing platforms.

Developing robust applications will also be crucial. As the number of applications for mobile systems and social networks continues to rise rapidly, the potential for malicious applications on those platforms will grow dramatically. Many application developers are from small business start-ups that create eye-catching applications on small budgets and are often willing to overlook security. Unfortunately, some device manufacturers or social media platforms have only a minimal, if any, application vetting process and may allow posting of applications that leave users exposed to vulnerable and/or malicious software. The good news is that this is changing. Looking to increase adoption in the enterprise, certain device manufacturers and social platforms are establishing more strict requirements to prove the viability and security of the applications, including the use of digital signatures to validate applications.

Great phishing on social sites

Cyber criminals continue to use social engineering to thwart security defenses and gain access into organizations. As social networking in the workplace rises, so does the availability of sensitive and private information on users, creating fertile ground for phishing attacks. Google's recent attack originating in China was perpetrated based on an elaborate social engineering scheme that began with extensive research on Google employees and leadership.[22] Criminals are using methods honed in the spamming world and adapting them; taking advantage of the speed and openness of individuals communicating via social media. Besides the risk that users will expose credentials, there is also the risk that users will get lured by fraudsters and recruited as money mules (individuals that transfer stolen money as a result of online scams). The best defense against phishers will be a well-educated user population.

When enabling a new innovation like user-driven IT to take root, it is impossible to gain rewards without taking risks. But it will be critical for the information security team to work closely with others across the company to make sure the enterprise is not taking undue risks.

"The risk inherent in any new technology is that you don't know what might happen. And you can try to forecast or foresee as much as you can, but if somebody figures out a way to exploit a vulnerability and there's no resolution for it, they're going to have a pretty large window to do things."

Dave Cullinane
Chief Information Security Officer and
Vice President
eBay

4. Get in Front of Technology Trends

To gauge the risks and rewards of user-driven IT, the security team will have to get up to speed on the consumer devices, applications and technologies that enable enterprise deployments. Most security organizations already analyze technical trends. However, now technologies are coming at a fast and furious pace. There is more newness to deal with than ever before; including a completely new computing paradigm – mobility. Eventually, the predominant computing platform that most people will use throughout the course of their day will be a mobile device. Some argue that this is similar to previous technology shifts when security personnel had to go from securing mainframes to personal computers; then from PCs to networked PCs on the Internet. Now they have to secure the mobile social web. Security professionals could be in for quite a ride.

Staying ahead of a fast moving target

Imagine three years ago trying to guess what smartphones would look like or where Facebook or Twitter would be today? And, as businesses vie for mind share on the mobile social web, the pace of change will continue to increase substantially. There is a veritable arms race as competitors try to outdo each other in designing and deploying mobile and social applications to drive business. According to IDC, iPhone applications are expected to grow 300 percent and Android applications 500 percent by the end of 2010.[23] As well, 86 percent of companies plan to spend more money on social media over 2010.[24]

In the consumer world, new apps are available constantly and entirely new gadgets are introduced every six months, but consumer technologies are not built with the enterprise in mind. Simple market dynamics mean that consumer functionality takes precedence over enterprise requirements since the consumer market is much larger. Therefore one of the challenges in enabling user-driven IT is that enterprise-grade features will always lag behind. For example, not all enterprise applications can even run on mobile devices. Data presentation issues will need to be solved. A case-in-point is the fact that Adobe Flash doesn't work on smartphones yet.

Desktop virtualization, thin computing and cloud computing are having a big impact on enabling mobile computing in the enterprise. The more processing that can be done in a centralized data center, the less has to be on the device, which helps to solve many of the security issues. However these computing technologies depend on having a fast and reliable Internet connection and available bandwidth.

Users may not always have connectivity; therefore new solutions such as distributed virtual desktops can provide access to applications even when users are not online. These solutions provide a fully-contained virtual corporate environment; corporate data can be protected and wiped off the mobile computer remotely if necessary, for example if the employee or contractor is terminated. There are also new mobile security and device management solutions for smartphones that enable enterprises to control access to and eliminate corporate data if necessary.

Security armory

Other security technologies could also play a pivotal role in enabling user-driven IT. For example, many organizations have adopted data loss prevention (DLP) solutions. Just as these solutions are currently used to help prevent data loss through communication methods like webmail, email and FTP as well as devices like USB and CD drives, they could be set up to stem the loss of important information via social networking or mobile devices.

"We have people in our security organization who keep on the bleeding edge of consumer technology. Through social media and gadget blogs, we try to get advance notice if something's coming, what it might look like, then watch for requests or see it start appearing on our networks. There are a lot of cycles involved in just keeping pace with the speed of change."

Dave Martin, Chief Security Officer, EMC Corporation

Enterprise rights management (ERM) also holds promise as an enabler of user-driven IT. So far, ERM has been limited to speciality applications. Requirements for a "next-generation" ERM solution include improved scalability, agility and better cross-platform support, including for mobile technology. Ideally it would provide an easy-to-use "wrapper" that could wrap itself around the data object independent of document format. Security officers will also have to figure out how to develop sound business processes for rights management.

Advanced authentication and trusted identity mechanisms will help facilitate access to more sensitive applications in mobile environments. For example, out-of-band authentication can be used to provide higher assurance on smartphones – before a user is allowed to conduct a higher-value transaction, they would receive a phone call and have to implement a PIN. Increasingly, trusted identity will include not only validating a trusted user, but also a trusted device. For example, authentication methods could check smartphones for malicious code like a virus, key logger, or screen scraper. Risk-based or adaptive authentication can match the level of assurance with the level of access; so that if a user wants deeper access to certain applications or content, granting that access will depend on higher levels of identity assurance and vetting of the device. The more a user is able to prove themselves and their device, the more access they'll get.

"When it comes to mobility, traditional IT security thinking is going to be blown apart because a smartphone does not have the same architecture as a PC. I think there are still significant numbers of IT security professionals who don't understand the new mobility platforms."

Professor Paul Dorey
Founder and Director, CSO Confidential and
Former Chief Information Security Officer, BP

To keep pace with all of the technology changes and find answers to technical issues, some information security organizations are opting for a dedicated individual or team focused on research and development (R&D). Other organizations will have various people devote a percentage of their time to R&D or rely more on external resources for the information on coming trends and emerging solutions. Whatever the approach, a system of periodic briefings or round tables can provide a forum for education and brainstorming on questions such as, "What if this particular technology comes to us? How are we are going to address it?" To really get ahead of the curve, actively develop a threat and risk catalogue for each of the technology areas you are considering and hold collaborative meetings on each major area to quickly educate the stakeholders on all aspects of the inherent risks.

New end-user experience architect lead

An exciting new development within security organizations is the creation of a new position – an end-user experience architecture lead. This position has evolved from having the traditional responsibilities for antivirus and content filtering. The role now also owns virtual desktop infrastructure (VDI) security, and is tasked with understanding what a secure mobile computing experience is going to look like for users. Paying attention to the user experience will be critical. If security procedures are too burdensome or too slow, then user productivity will suffer or users will just find ways to go around them.

"Some of the significant technical issues around mobility will be delivering meaningful enterprise applications and the appropriate security controls on such a small form factor.

Roland Cloutier
Vice President, Chief Security Officer
Automatic Data Processing, Inc.

"To enable mobile devices to access corporate services, it's all about content and where does the content stay. Providing visibility to the content through a remote desktop session is much more palatable for enterprises than say, letting users pull down a database onto their smartphone or personal PC."

David Kent
Vice President
Global Risk and Business Resources, Genzyme

5. Own the Future

Information security leaders have always been tasked with protecting the environment of today while planning for tomorrow. But throwing consumer technologies into the mix adds some new challenges. In this rapidly changing world, it is possible that by the time an information risk management strategy is planned and implemented, business or technical requirements will have changed and the strategy will be outdated. The ability to anticipate changes before they happen will be more important than ever.

A cross-functional team will help cover all the angles. First and foremost, information security will be working very closely with members of the IT team to understand technology trends and architect solutions. Other key partners in this endeavor will include legal, for establishing policy and user agreements, etc.; human resources and compliance for developing user training; and finance for making investments and creating compensation models.

Information security is a crucial element of enabling user-driven IT; but it is only one element. For example in most enterprises today, the service-level agreements, vendor contracts and support structures are all geared toward the preeminent model whereby enterprise IT controls end-user technologies. New service models will have to be created; licensing contracts re-negotiated; new infrastructure deployed as well as new financial compensation models devised (such as stipends for users to buy their own machines). Support mechanisms will have to be carefully planned; for example, the help desk cannot be expected to suddenly support every type of mobile device under the sun or costs will skyrocket.

User-driven IT makes budgeting for security trickier than ever. Consumer technologies can change faster than traditional budgeting models allow. Once a budget is in place for the year ahead, it could be difficult to change if new requirements develop. Waiting for the new budget cycle could mean increased risk and missed opportunity for the business. In addition, this all comes at the same time as other major IT initiatives like cloud computing. Flexible budgets with built-in contingency funds can help meet future demands; and creating operational efficiencies can free-up resources for future investments.

To really know what user-driven IT involves, it will be essential for the extended team to gain experience through pilots and small deployments. Pick a starting point – know which user groups and applications would be good initial projects. Be able to sniff out real business cases versus user demands based on preferences only. Know where there is manageable risk. For example, for the first projects you may want to steer clear of any applications involving sensitive or regulated data. Make sure that specific user training is part of any pilot project. These initial test projects in user-driven IT will be key to knowing what the future looks like.

"Unfortunately you don't know what it is that you're trying to secure because you don't know what's coming out. I always tell my team that one of the characteristics that makes a good security person is flexibility and agility. You have to be able to quickly move in time to where the technology is going."

Dr. Claudia Natanson
Chief Information Security Officer
Diageo

"Security needs to understand each environment – what are the capabilities and limitations? What are the vulnerabilities? What are the attack surfaces? What are your options for mitigating them? Do you have the right tools to mitigate them? If you don't, where are you going to get the money to do that?"

Dave Cullinane
Chief Information Security Officer
and Vice President
eBay

Examples of real-world pilots and deployments*

Corporate app for the iPhone® mobile digital device

- Employees allowed to access SAP requisition approvals and Business Objects reporting with personal smartphones
- Did not expose sensitive or regulated data
- Started small, kept it simple, few applications and limited user group

"Bring your own computer" deployment for contractors

- Objective was to allow thousands of contractors to use their own PCs because cost of issuing hardened laptops too high
- Mandatory training and legal agreements were required
- Enabled by virtual machine on USB drive
- Full responsibility of device management and support moved to end-user

Integrated personal/corporate machine for road warriors

- Employees enabled to carry one device for both personal and corporate use
- Virtualization technology partitioned corporate/ personal data

Increased access to social media

- Targeted specific user groups with business need
- Provided extensive user training to enable users to understand risks and responsibilities

Tablet pilot

- Company equipping one hundred executives with tablets
- Program to test if the tablet can withstand being loaded with corporate apps and data

*Examples from Council members and their peers

6. Collaborate with Vendors

In an environment where technology is moving rapidly, working closely with vendors is essential. Build collaborative relationships with vendors of consumer and enabling technologies. Knowing mobile device and social media vendors' plans is critical to knowing what the user computing experience will look like. Work with vendors to understand what is on the horizon, and also to provide input into enterprise requirements and time frames.

The telecommunications companies could play a key role in enabling user-driven IT. They control the mobile networks and connectivity to those networks, and have the ability to manage the devices. For example, they can reconfigure a phone, track its traffic, cancel a call, and provide updates and patches to the device. As they increase capacity and bandwidth, they also have the ability to add important services for the enterprise community. One such valuable service could be device integrity services, whereby the mobile device would be guaranteed to be "healthy," including all necessary security patches. "Telco 2.0", the telecom parallel to Mobile 2.0, (driven by GSM Association, the largest mobile telecoms body), has defined Identity, Authentication and Security services as a major business opportunity for growth.[25] In this role the carriers, considered to be experienced, trusted entities, could provide identity verification services and would validate the safety of the environment – as a result dramatically increasing the confidence of the mobile platform for the enterprise.

The social platform vendors have control over all the data that is being transferred between their millions of subscribers; they also have an aggressive strategic plan to deliver enterprise focused functionality. It is imperative that security organizations work with these vendors to influence the roadmap as well as their data ownership and privacy policies. For example, Facebook's recent changes to their privacy settings have generated substantial reaction in the marketplace. Security organizations should work with Facebook and other social platforms to help them devise privacy settings to protect enterprise and user privacy. In addition, these vendors, along with mobile device vendors, have the ability (and responsibility) to control the quality and "readiness" of the applications deployed on their platforms. Information security teams should provide input into their formal vetting process for testing and validating applications to help mitigate the risk of malicious and malware-susceptible applications that can easily penetrate the enterprise. Organizations must work with these vendors to demand a process that will result in applications that can be trusted.

Of course, as security teams are challenged with an onslaught of new potential risks, they need to continue to work closely with security vendors. Some of the challenges can be tackled with mobile versions of traditional security solutions such as data leakage and intrusion prevention tools. However, many of the risks will require new products. Security leaders need to see what is on their vendors' drawing boards and collaborate with them to develop enterprise-class solutions that address the needs of enterprise security.

Collaborating with a wide array of vendors to ensure solutions to such a broad range of challenges is not easy. Clearly, no single enterprise has the ability, resources, or influence to steer the industry in any given direction. For that reason, several organizations have expressed the need for a community forum to define the "Secure Mobile Social Web." This would be focused on ensuring that the user experience -including the devices, applications, enabling and security technologies – would work to provide a secure and seamless mobile social web experience for maximum user productivity and optimum data protection. With representation from enterprises and vendors, it would develop best practices for enabling user-driven enterprise IT and facilitate communication so that vendors can provide the functionality the enterprise needs to smooth the adoption of these new computing technologies.

Conclusion

Rather than viewing the inevitable movement toward user-driven IT as a threat to their control, information security teams can use it as an opportunity to bolster their own value. For enterprises to reap the rewards, they have to be able to manage the risks. Meeting the challenges of user-driven IT demands information security teams work to enable innovation at an accelerated pace. The good news is that most teams are not starting from scratch. After several years focused on business alignment, most information security organizations have the "right stuff" to tackle user-driven IT; and they have a lot of resources on which to draw.

Besides this report, the previous reports from the "Security for Business Innovation Council"[26] provide relevant guidance for information security teams. They cover many aspects of how to operate at high speeds such as:

- Get attuned to the business. See *"The Time is Now: Making Information Security Strategic to Business Innovation"*
- Create self-assessment and repeatable processes for managing risk. See *"Mastering the Risk/Reward Equation: Optimizing Information Risks to Maximize Business Innovation Rewards"*
- Focus on measuring and improving productivity while increasing efficiencies. See *"Driving Fast and Forward: Managing Information Security for Strategic Advantage in a Tough Economy"*
- Enable secure collaboration among all of the various constituencies across the enterprise. See *"Charting the Path: Enabling the 'Hyper-Extended' Enterprise in the Face of Unprecedented Risk"*
- And to really grease the wheels, get executive leadership on your side. See *"Bridging the CEO-CISO Divide"*

The information security teams that successfully navigate this sea change will be best positioned to make the right judgment calls about where, when and how to embrace consumer technologies to create rich new sources of competitive advantage and business return for their organizations.

"The trend toward leveraging non-corporate-controlled assets and using social media for accessing and distributing information – is inevitable. It would be a mistake for any company to put its head in the sand or to dig its heels; because the tide will be working against you. It would be much better to recognize it and then create the parameters to make it work for you."

David Kent
Vice President, Global Risk and Business Resources
Genzyme

Security for Business Innovation Council Members

Anish Bhimani, CISSP,
Chief Information Risk Officer
JPMorgan Chase

Anish has global responsibility for ensuring the security and resiliency of JPMorgan Chase's IT infrastructure and supports the firm's Corporate Risk Management program. Previously, he held senior roles at Booz Allen Hamilton and Global Integrity Corporation and Predictive Systems. Anish was selected "Information Security Executive of the Year for 2008" by the Executive Alliance and named to Bank Technology News' "Top Innovators of 2008" list. He authored "Internet Security for Business" and is a graduate of Brown and Carnegie-Mellon Universities.

Bill Boni, CISM, CPP, CISA
Corporate Information Security Officer,
VP Enterprise Information Security
T-Mobile USA

An information protection specialist for 30 years, Bill joined T-Mobile in 2009. Previously he was Corporate Security Officer of Motorola Asset Protection Services. Throughout his career Bill has helped organizations design and implement cost-effective programs to protect both tangible and intangible assets. He pioneered the application of computer forensics and intrusion detection to deal with incidents directed against electronic business systems. Bill was awarded CSO Magazine's "Compass Award" and "Information Security Executive of the Year – Central" in 2007.

Roland Cloutier
Vice President,
Chief Security Officer,
Automatic Data Processing, Inc.

Roland has functional and operational responsibility for ADP's information, risk and crisis management; and investigative security operations worldwide. Previously, he was CSO at EMC and held executive positions with consulting and managed services firms. He has significant experience in government and law enforcement, having served in the U.S. Air Force during the Gulf War and later in federal law enforcement agencies. Roland is a member of High Tech Crime Investigations Association, State Department Partnership for Critical Infrastructure Security and Infragard.

Dave Cullinane
Chief Information Security Officer
and Vice President, eBay

Dave has more than 30 years of security experience. Prior to joining eBay, Dave was the CISO for Washington Mutual and held leadership positions in security at nCipher, Sun Life and Digital Equipment Corporation.

Dave is involved with many industry associations including as current Past International President of ISSA. He has numerous awards including SC Magazine's Global Award as CSO of the Year for 2005 and CSO Magazine's 2006 Compass Award as a "Visionary Leader of the Security Profession."

Security for Business Innovation Council Members

Professor Paul Dorey
Founder and Director, CSO Confidential and Former Chief Information Security Officer, BP

Paul is engaged in consultancy, training and research to help vendors, end-user companies and governments in developing their security strategies. Before founding CSO Confidential, Paul was responsible for IT Security and Information and Records Management at BP. Previously, he ran security and risk management at Morgan Grenfell and Barclays Bank. Paul was a founder of the Jericho Forum, is Chairman of the Institute of Information Security Professionals and a Visiting Professor at Royal Holloway College, University of London.

Renee Guttmann
Vice President, Information Security & Privacy Officer,
Time Warner Inc.

Renee is responsible for establishing an information risk-management program that advances Time Warner's business strategies for data protection. She has been an information security practitioner since 1996. Previously, she led the Information Security Team at Time Inc., was a security analyst for Gartner and worked in information security at Capital One and Glaxo Wellcome. Renee received the 2008 Compass Award from CSO Magazine and in 2007 was named a "Woman of Influence" by the Executive Women's Forum.

David Kent
Vice President, Global Risk and Business Resources,
Genzyme

David is responsible for the design and management of Genzyme's business-aligned global security program, which provides Physical, Information, IT and Product Security along with Business Continuity and Crisis Management. Previously, he was with Bolt Beranek and Newman Inc. David has 25 years of experience aligning security with business goals. He received CSO Magazine's 2006 "Compass Award" for visionary leadership in the Security Field. David holds a Master's degree in Management and a Bachelor of Science in Criminal Justice.

Dave Martin, CISSP
Chief Security Officer,
EMC Corporation

Dave is responsible for managing EMC's industry-leading Global Security Organization (GSO) focused on protecting the company's multi-billion dollar assets and revenue. Previously, he led EMC's Office of Information Security, responsible for protecting the global digital enterprise. Prior to joining EMC in 2004 Dave built and led security consulting organizations focused on critical infrastructure, technology, banking and healthcare verticals. He holds a B.S. in Manufacturing Systems Engineering from the University of Hertfordshire in the U.K.

Security for Business Innovation Council Members

Dr. Claudia Natanson
Chief Information Security Officer,
Diageo

Claudia sets the strategy, policy and processes for information security across Diageo's global and divergent markets. Previously, she was Head of Secure Business Service at British Telecom, where she founded the UK's first commercial globally accredited Computer Emergency Response Team. Claudia is Chair of the Corporate Executive Programme of the World Forum of Incident Response and Security Teams. She holds an MSc. in Computer Science and a Ph.D. in Computers and Education.

Vishal Salvi, CISM
Chief Information Security Officer
and Senior Vice President,
HDFC Bank Limited

Vishal is responsible for driving the Information Security strategy and its implementation across HDFC Bank and its subsidiaries. Prior to HDFC he headed Global Operational Information Security for Standard Chartered Bank (SCB) where he also worked in IT Service Delivery, Governance & Risk Management. Previously, Vishal worked at Crompton Greaves, Development Credit Bank and Global Trust Bank. He holds a Bachelors of Engineering degree in Computers and a Masters in Business Administration in Finance from NMIMS University.

Craig Shumard
Chief Information Security Officer,
CIGNA Corporation

Craig is responsible for corporate-wide information protection at CIGNA. He received the 2005 Information Security Executive of the Year Tri-State Award and under his leadership CIGNA was ranked first in IT Security in the 2006 Information Week 500. A recognized thought leader, he has been featured in The Wall Street Journal and InformationWeek. Previously, Craig held many positions at CIGNA including Assistant VP of International Systems and Year 2000 Audit Director. He is a graduate of Bethany College.

Denise Wood
Chief Information Security Officer
and Corporate Vice President,
FedEx Corporation

Denise is responsible for security and business continuity strategies, processes and technologies that secure FedEx as a trusted business partner. Since joining in 1984 she has held several Information Technology officer positions supporting key corporate initiatives, including development of fedex.com; and was the first Chief Information Officer for FedEx Asia Pacific in 1995. Prior to FedEx, Denise worked for Bell South, AT&T and U.S. West. Denise was a recipient of Computerworld's "Premier 100 IT Leaders for 2007" award.

References

1. *"Smartphone Management Survey: An Enterprise IT Operations Perspective",* BoxTone and eMedia, April 2010
2. *"Gartner Survey Shows 10 Percent of Respondents Say Workers Using Employee-Owned Notebooks as Their Primary Work PC in 2009",* Gartner Press Release, December 7, 2009
3. *"BYOC: Kraft Foods Employees Can Now Bring Their Own Computers to Work",* Yahoo! Finance, May 11, 2010
4. *"e-Bay Expands into iPhone Apps",* American Consumer News, March 30, 2010
5. *"Understanding Enterprise Mobility Trends and Mobile Usage",* The iPass Mobile Workforce Report, February 2010
6. *"Smartphone Surge Offers Opportunities for Business",* IT Business Edge, March 11, 2010
7. *Number of Mobile Devices Accessing the Internet Expected to Surpass One Billion by 2013,* IDC Press Release, December 9, 2009
8. *"Facebook Crosses the 500-Million Threshold, ComScore Says",* WSJ Blog, May 18, 2010
9. *"Biz Stone: Twitter has 105 million users",* MacWorld, April 14, 2010
10. *Frequently Asked Questions,* Linkedin.com, May 2010
11. *"Facebook and YouTube dominate workplace traffic and bandwidth",* SC Magazine, April 16, 2009
12. *"57% of US Workers Use Social Media for Business Purposes",* Social Media at Work, January 26, 2010
13. *"Social Media Statistics"* Socialware Compass, 2010
14. *"5 B2B Social Media Winners",* TopRank Online Marketing Blog, February 11, 2010
15. *"Gartner Reveals Five Social Software Predictions for 2010 and Beyond"* Gartner Press Release February 2, 2010
16. *"Mastering the Risk/Reward Equation: Optimizing Information Risks to Maximize Business Innovation Rewards",* Security for Business Innovation Council Report
17. *"Fact Sheet 7: Workplace Privacy and Employee Monitoring",* Privacy Rights Clearinghouse (PRC), April 2010
18. *"Sexy New Mobile Botnet on the Move?",* eWeek Security Watch, July 17, 2009
19. *"Imminent flood of smartphone malware?",* Net Security, February 18, 2010
20. *"Mac OS X Trojan Found in Pirated Photoshop CS4",* Information Week, January 26, 2009
21. *"Malware and spam rise 70% on social networks, security report reveals",* Sophos, February 1, 2010
22. *"Hackers target friends of Google workers",* Financial Times (FT.com), January 25, 2010
23. *"IDC Predicts Recovery and Transformation in 2010* – Modest IT Spending Growth to be Accompanied by Fundamental Industry Transformation", IDC Press Release, December 3, 2009
24. *"86% of Companies Plan Social Media Budget Bumps",* Bigmouth Media, December 4, 2009
25. *"Telco 2.0™ Manifesto",* Telco2.net, 2010
26. For the Security for Business Innovation Report Series Go to www.rsa.com/securityforinnovation
27. http://www.facebook.com/brandpermissions/index.php
28. http://help.twitter.com/entries/77641-guidelines-for-use-of-the-twitter-trademark
29. http://homepage.mac.com/haydock/mfn/steeringcommittee/group_services_agreement.pdf
30. http://na.blackberry.com/legal/trademarks.jsp#tab_tab_guidelines
31. http://www.google.com/permissions/guidelines.html

RSA®

The Security Division of EMC

www.rsa.com

CISO RPT 0710