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"

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

This synopsis is a small teaser of the wealth of information provided by the Security for Business Innovation Council. For a deeper dive, please view the full report at www.rsa.com/securityforinnovation.

User-Driven IT Taking Hold in the Enterprise

An unstoppable force is knocking at the doors of enterprise IT departments worldwide. Users are demanding a voice. They want to choose the technologies that will make them most productive and bring them into the enterprise. The traditional model whereby IT dictates all of the technology used in the enterprise is quickly crumbling.

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.

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?" 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 application from their smartphones while they are on the road. Executives want smartphone access to approve travel expenses and purchase orders.

Rewards versus Risks

The potential rewards of user-driven IT are 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 microblogging 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.

Re-Calibrating Information Security

The enterprises that 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.

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.

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 with the potential of decreased costs and increased revenue. 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.

The Roadmap

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 including 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. 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.

> "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

> “The demand keeps building and building. Meanwhile information security is doing research trying to figure out the requirements. You have to be 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

1. Shift Minds to the Times

As users increasingly make decisions about how technology is used in the enterprise, security teams must shift their attitudes from command and control to oversight and business enablement. 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.”

2. Reframe Users as Assets

The average person has become a sophisticated technology user. 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. Think of your user population as a powerful tech-savvy army that can help educate you about the latest gadgets and applications.

Instead of treating user education as one-way communication, security needs to re-invent it as a two-way conversation. Listen carefully to what users want to do and determine which requests could translate into real business value. 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. Make the tradeoffs clear: more choice means more responsibilities.

3. Support Calculated Risk-Taking

Consumer technologies represent enormous opportunity, but there are still many uncertainties about the risks. In the legal and compliance realm, there are issues around ownership and representation, e-discovery and privacy. There are also escalating threats including mobile malware, sophisticated social engineering and targeted phishing attacks. 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.

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 consumer devices and applications as well as the technologies that enable enterprise deployments. Pivotal enablers include virtualization, thin computing, cloud computing, and security technologies such as advanced authentication and data loss prevention.

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 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.

5. Own the Future

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.

Organizationally, building a cross-functional team will help cover all the angles: in addition to working very closely with IT, other key partners in this endeavor will include legal, human resources and compliance and finance. Operationally, establishing flexible budgets with built-in

contingency funds can help meet future demands and creating efficiencies can free-up resources for future investments. Practically, to really know what user-driven IT involves, it will be essential for the extended team to gain experience through pilots and small deployments.

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.

Embrace the Opportunity

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. 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 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 the organization could be put at great risk.

At RSA, 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.

www.rsa.com

CISO6_SYN_0710