

# TREND

## ADVISORY

### INFORMATION-CENTRIC SECURITY

Confronting the Threats to Your Network

- 01 RISK AND REWARD IN THE INFORMATION AGE**  
The imperative to have security keep pace with innovation
- 02 NOT ALL DATA IS CREATED EQUAL**  
Learn how to classify your information
- 03 SECURITY THAT CAN REALLY MOVE**  
Data moves, so security should move with it
- 04 BEYOND THE BOX**  
CDW assesses your needs and implements and supports your security solution



**229,441,775**

THE TOTAL NUMBER OF RECORDS EXPOSED IN SECURITY BREACHES  
IN THE UNITED STATES BETWEEN JANUARY 2005 AND JUNE 2008

*(Privacy Rights Clearinghouse)*

**\$197**

THE AVERAGE COST PER RECORD OF A SECURITY BREACH

*(Ponemon Institute, "2007 Annual Study: U.S. Cost of a Data Breach")*

**\$6.3 MILLION**

THE AVERAGE TOTAL COST OF A SECURITY BREACH

*(Ponemon Institute, "2007 Annual Study: U.S. Cost of a Data Breach")*

# RISK AND REWARD IN THE INFORMATION AGE

NETWORKS HAVE BECOME MORE OPEN AND INTERCONNECTED. EMPLOYEES,  
PARTNERS AND CUSTOMERS EXCHANGE INFORMATION FREELY, FUELING CREATIVITY  
AND INNOVATION. THOUGH GOOD FOR THE BOTTOM LINE, THESE CHANGES HAVE  
BLURRED THE BOUNDARY BETWEEN THE NETWORK AND THE OUTSIDE WORLD —  
FORCING COMPANIES TO RETHINK THEIR APPROACH TO SECURITY.

Information travels faster and to more people than ever before — far beyond the safety of your firewall. Employees routinely access information on the road, using a growing variety of mobile devices to connect to the network. The network has also opened up to business partners, suppliers and distributors, letting companies share information to an unprecedented degree. And then there's the Internet, providing a channel for your information to reach the world at large.

With so many access points, the network can become a minefield of vulnerabilities. Every notebook, personal digital assistant (PDA) and USB stick is a potential entry point for viruses, worms and spyware. And with so much activity outside the perimeter, you can easily lose control of confidential data. Employees may violate corporate policies, either intentionally or accidentally. Notebooks can be lost or stolen. The consequences can be dire. If customer information is compromised, your company can be held legally liable and may have to pay regulatory fines. You can also lose a competitive advantage if proprietary information falls into the wrong hands.

## **THINK BEYOND THE PERIMETER**

Faced with these risks, you may be tempted to simply rein in the access points and build a thick wall around the network. Resist the temptation. A strong perimeter may help guard against

intrusion, but it can also keep information locked away from the people who need it. And that can stifle productivity, innovation and growth. If you're wondering what the alternative is, it's probably time to take a step back and reassess your security strategy.

## **BIND SECURITY TO INFORMATION — WHEREVER IT GOES**

Information is in a constant state of flux. In the blink of an eye, it can jump from San Francisco to Bangladesh. It can change from a database record to a PDF file. It can materialize suddenly on thousands of notebooks around the world. And the content is always evolving. To keep up with the fluid, dynamic nature of information, you need to take an information-centric approach to security.

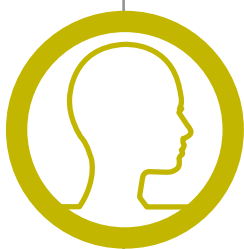
An information-centric security strategy gives business users the freedom to access information when and where they need it while protecting against intrusion, data loss or misuse of company information. The key is to attach security measures to information, rather than to systems. That way, the information behind the network perimeter — and the information that ventures beyond it — stays safe, even if mobile devices fall into the wrong hands or if access points are compromised.

# NOT ALL DATA IS CREATED EQUAL

---

An information-centric security strategy requires a thorough understanding of the data your company creates, stores and uses — and what role it plays in the business. In other words, you need to understand what you're protecting to determine how to protect it. Not all information warrants a full security detail. Other information, such as customer records, human resources data and financial statements, may be worth the cost of maintaining several layers of security. Knowing the difference can help you prioritize your security initiatives and establish specific, granular policies that give access to all the right people at the right times — and keep the wrong ones out.

## GET TO KNOW YOUR INFORMATION



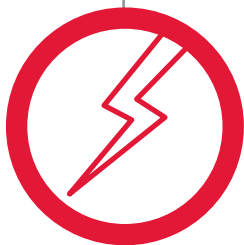
**Who uses it?** This is a good place to start. Understanding the users — including their quantity, location and job functions — can give you a good sense of how much accessibility is needed in each area. For instance, information that is used only by a core group of accountants at your headquarters will require much less sophisticated security measures than information accessed by a global sales force and third-party distributors.



**How is it used?** Data is worth saving and securing only if it fulfills some business function. Your task is to identify which is which, so you can match information with appropriate security measures. In the process, you may discover that some data is insufficiently protected. Customer records often turn up in this category because of their frequent use and integration with online systems.



**Where does it live?** Information often resides in multiple places: the server, desktop computers, storage devices, partner systems and websites. If it is important enough to protect on the server, it is important enough to protect everywhere it lives.



**What are the risks involved?** Identify the potential threats to your information. Determine how much damage a security breach would cause, in terms of financial loss, legal liability, regulatory fines, lost opportunities and damage to the company's reputation. Your security efforts should focus first and foremost on the most vulnerable and most sensitive information.



# SECURITY THAT CAN REALLY MOVE

Information doesn't just sit idle. Much of it is in constant motion — carried on mobile devices, downloaded from the Internet, saved on hard drives and transmitted through e-mail. Information-centric security must establish safeguards at every point of its journey. There are two basic categories to consider when assigning security tactics.

## **INFORMATION AT REST: PROTECTING DATA WHERE IT LIVES**

The growing number of network access points puts information at risk, even when it sits behind the perimeter. Lost or stolen mobile devices can provide an open door into the network. And even authorized users may abuse their access rights. To keep it from happening, you need to protect data at the source — blocking both unauthorized users and unwanted behavior. How?

- **Network access control (NAC):** Restrict network access for endpoints
- **Database access control:** Limit users' ability to view and modify data
- **Risk-based authentication:** Require users to log in

## **INFORMATION IN TRANSIT: PROTECTING DATA WHEREVER IT GOES**

E-mail, instant messaging, FTP sites, thumb drives — they all make it easy to pass information around. In fact, information travels so far and wide that companies often lose track of how it gets used and who sees it. Messages can be intercepted. Documents can be copied. Portable storage devices can be co-opted. To regain control, you must send security along for the ride. How?

- **Data leakage protection:** Restrict the ability to copy, print, save or transmit data
- **E-mail encryption:** Make sure that only the intended recipient can read it
- **Hard disk encryption:** Keep unauthorized users from accessing stolen equipment
- **Security tokens:** Issue one-time passwords at every log in
- **Patch management:** Automate security patch updates on endpoints

## BEYOND THE BOX:

# OUR APPROACH TO SECURITY

At CDW, you'll find the experience and the technology you need to adopt an information-centric security strategy. Our 20 years of experience have taught us that personal support is a must — from beginning to end. That's why we dedicate an account manager to act as a central point of contact and your conduit into our network of certified specialists, expert field engineers and top vendors.

Every CDW solution includes a security assessment and design; hardware and software configuration; integration; and support. Our dedicated security specialists will help assess your security landscape — either onsite or over the phone — to determine what you have, what you need and how to deliver the best solution that fits with your budget. We'll even help you calculate the potential cost savings and return on investment (ROI).

Once we find a plan that works for your business, CDW will help you implement it. We configure your solution, so it's ready to deploy, right out of the box. If you need onsite assistance, we'll be there. And you can rely on ongoing support to make sure everything works as planned.

### A BRIEF CHECKLIST FOR YOUR INFORMATION SECURITY STRATEGY

- Classify your information
- Define a security policy that addresses data access, user responsibilities and compliance issues
- Document a response procedure to ensure proper handling of security breaches
- Communicate information security policies to employees
- Establish a system for performing regular software updates and deploying unscheduled security patches
- Define a process for introducing new hardware into the security landscape; dispose of old hardware carefully
- Take stock of the mobile devices that access the network
- Refresh passwords and encryption keys frequently

With CDW, you have a partner in technology and support from a network of experts.

## YOUR CDW SECURITY AND STORAGE TEAMS

EXPERTISE TO GET YOU TO THE RIGHT SOLUTION

When it comes to your IT environment, knowing what to do and how to do it is more important than the products you install. Whether it's security or storage, your IT initiatives must be guided by sound strategy, attention to business objectives and an understanding of how technologies work together. At CDW, our specialists offer the expertise you need to adopt a measured, effective approach to storing and protecting your critical information.



**JEFFREY A. FALCON**  
SECURITY SPECIALIST, NETWORK SECURITY PRACTICE, CISSP

With eight years of experience helping customers overcome their security challenges, I've learned how important it is to put their business needs first. That's why I recommend taking the time to assess your business objectives with CDW's assessment and compliance consulting services. Our knowledge of best-of-breed products, relationships with manufacturers and expertise in the design and implementation of complex solutions can help you adopt a mature, competitive network security practice.



**BRUCE MODELL**  
ENTERPRISE STORAGE SPECIALIST, VCP, CCDA, CCSE, EMC SE, SERVER +

In my 13 years at CDW, I've helped build the Storage Specialty Group from the ground up — making sure to uphold our brand-agnostic approach to solutions. You can count on an unbiased recommendation, whether or not we sell the products in question. I also personally recommend using the various Web-based learning modules offered by many storage vendors to find out more about the storage technologies available to you.

## BEST PRACTICES

Here are a few things to think about when planning an information-centric security strategy.

- ❑ **DO:** Establish security policies that define access rights for different user profiles
- ❑ **DON'T:** Assume that your network is secure just because only authorized users have access; be sure to monitor behavior during network sessions to detect policy violations
- ❑ **DO:** Allow mobile devices and other remote endpoints to access the network
- ❑ **DON'T:** Relinquish control over security updates on remote endpoints

# CDW SELECTS

In addition to incorporating leading hardware and software, CDW solutions automatically include experience and support. Our security specialists work closely with you and your account manager to provide a practical, reliable approach for protecting your critical information.



The Security Division of EMC

## RSA SECURID®

### A reliable level of user authentication

Positively identify users before they interact with mission-critical data and applications through:

- VPNs, WLANs and e-mail
- Intranets and extranets
- Microsoft® Windows® desktops
- Web servers

### Call for pricing¹

**RSA SecurID Appliance**  
CDW 854205



**RSA SecurID Software**  
CDW 799449



¹Maintenance sold separately



## PGP® WHOLE DISK ENCRYPTION

### Comprehensive mobile security for notebooks, desktops, external drives and USB Flash drives

- Provides secure, comprehensive disk encryption that is nonstop and user-transparent
- Encrypts everything on the hard disk, including data files, system files, temporary files and applications data
- Enables professionals to quickly and cost-effectively provide powerful data security, immediately safeguarding sensitive information from unauthorized access
- Complies with existing and emerging industry and government regulations for information security and partner data protection requirements

### Call for pricing

**100-499 users**  
CDW 1079399



## EMC CLARIION® AX4 WITH INTEL® XEON® PROCESSORS

### Easy to use, affordable networked storage

Keep your company's critical information available and safe. The EMC® CLARiiON® AX4 is ideal for medium-sized businesses and commercial customers seeking to consolidate storage for the first time, and will scale as your business grows. Easy-to-use management software and renowned CLARiiON high availability make the AX4 the right choice for your business, not to mention easy on your budget.

- Consolidate Windows, Linux® and major UNIX® servers
- VMware®-certified solution with powerful Intel® Xeon® processors
- Scales as your VMware environment grows from 1.2TB to 60TB and 64 hosts
- Opt for iSCSI or Fibre Channel connectivity
- Mix and match SATA and SAS drives for varying application requirements

### Call for pricing

CDW 1438999



Starting at  
**\$8599**

To discuss an information-centric security solution designed for your business, call your CDW account manager today or **800.985.4239**

The terms and conditions of product sales are limited to those contained on CDW's website at CDW.com; notice of objection to and rejection of any additional or different terms in any other form delivered by customer is hereby given; CDW®, CDW•G® and The Right Technology. Right Away.® are registered trademarks of CDW Corporation; all other trademarks and registered trademarks are the sole property of their respective owners

