CDW·G® PEOPLE WHO GET IT™

I.T. SECURITY: INVESTMENT STRATEGIES

As cyberthreats continue to grow, strategic investments in IT security tools will help government organizations protect their information assets.

Executive Summary

In today's cyberthreat environment, an important challenge facing any government CIO, CISO or other IT decision-maker is convincing executive management to invest more in IT security. Threats have evolved; so have IT priorities. As a result, chances are high that the defense technologies an agency purchased when the strategic focus was defending the network (firewalls, intrusion prevention systems and so on) won't keep today's threats at bay or keep an agency's most critical IT asset – its data – completely safe.

To complicate matters, agencies at the federal, state and local levels are being encouraged to capture, store and analyze much more data – Big Data – and use it effectively to carry out their missions. Moreover, where that data resides and how it's accessed have evolved as well.

SHARE THIS WHITE PAPER

Table of Contents

Plus, the network isn't what it used to be. E-government initiatives encourage citizens to interact with government online to ensure better service; mobile computing enables telework programs that give workers access to IT resources from home and on the road; and emerging bring-your-own-device (BYOD) programs grant government employees access to agency data via personal smartphones and tablets.

In all these cases, the traditional network endpoint (the point at which data is viewed and acted upon) has been redefined. Federal, state and local IT security professionals couldn't envision the threats that such developments would bring when they were busy securing the network perimeter.

None of this is to say that prior investments in IT security have been for naught. But as cyberthreats evolve in conjunction with a growing interest in providing open access to data for citizen services, agencies must keep up with how they protect their critical assets.

Investing in new security solutions now, before a breach occurs, is better than waiting to react, because risk is a moving target. What emerges as a security risk tomorrow may not be a risk today. To build a complete line of defense, agencies must consider steps such as continuous monitoring, mobile device management (MDM), encryption and data loss prevention (DLP), in addition to traditional security solutions.

The State of Information Security in Government

Government agencies have become increasingly dependent on data — creating, collecting and making sense of it. At the same time, the "bad guys," whether joyriding hackers, hacktivists, cybercriminals or unfriendly nations, are equally interested in this data, from passwords and financial records to Social Security numbers and classified files.

In February 2013, President Obama issued an executive order that read in part, "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."

Government organizations need to better understand the threats they face and improve information security, and they must do so in a time of reduced or flat IT budgets. Greater efficiencies are needed to offset reduced staffing and services that are a result of budgetary curtailing. But it can be accomplished, provided the IT and security teams plan accordingly and invest in solutions that address the most pertinent threats.

In a report issued the same month as the president's executive order, the U.S. Government Accountability Office (GAO) reported that only eight out of 22 major federal agencies (down from 13 a year earlier) were in compliance with risk-management requirements under the Federal Information Security Management Act (FISMA) — a foreboding sign.

When it comes to effective investment in IT security, assessing risk is critical. If a government organization doesn't know what to protect, why and from whom, then it can't know if it has the proper security solutions in place. And if that's the case, it's just a matter of time before an agency suffers another security breach.

Over a period of six years, the number of security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) jumped to 48,562 in 2012. That's up from 5,503 in 2006.

Of the security incidents reported to US-CERT in fiscal year 2012:

- 37% were under investigation
- 20% involved violating agency IT policies
- 18% involved malicious code
- 17% were for unauthorized access
- 8% were the result of scans, probes or attempted access

And vulnerabilities permeate all levels of government. In a 2012 cybersecurity study coproduced with Deloitte, the National Association of State CIOs (NASCIO) found that 70 percent of state CISOs had reported an IT security breach. In the same study, only 24 percent of state CISOs said they were very confident about protecting their state's assets from external threats.

None of this should come as a surprise. More people are trying to break into government IT systems for more reasons than ever before. The once-stereotypical young hacker has been supplanted by shadowy players, such as organized crime syndicates, nation states bent on espionage and hacktivists, who attack networks and expose data as a political statement. Even government workers or contractors may be responsible for security breaches (such as the recent National Security Agency-PRISM scandal), whether deliberate or inadvertent.

CASE STUDY

Next-Generation Firewalls Simplify Security for Agencies

Feds report more visibility and enhanced application control from the latest crop of firewalls.

Next-gen Firewalls Simplify Security

Learn how next generation firewall capabilities are helping agencies simplify their security strategies:

CDWG.com/secureinvest1

The rise of a mobile workforce has ushered in a commensurate rise in unintended security breaches. On one end of the spectrum are incidents in which otherwise well-meaning employees load sensitive data onto devices and then lose those devices.

In 2012, for example, the NASA inspector general told Congress that the agency had lost 48 mobile devices between April 2009 and April 2011, some of which held sensitive data. On the other end of the spectrum is a tide of malware aimed specifically at mobile devices (notebooks, tablets and smartphones) that are inherently less secure than desktops and servers. According to the GAO, mobile malware grew 185 percent between July 2011 and May 2012.

In the face of this onslaught, it's no longer enough for government agencies to strive to keep threats out of their networks. New security solutions are required to protect data wherever and however it's made available. Organizations today must erect defenses, assume they will eventually be breached, and ensure that they have systems in place to respond quickly, mitigate or eliminate the threat, and then minimize the damage.

Why is this especially important now? Because even as government agencies acknowledge new and dynamic IT security threats, they plan to rely even more on IT and enterprise data to carry out modern missions:

- In 2012, the Obama Administration announced its Big Data Research and Development Initiative to encourage new ways of collecting, storing, analyzing and sharing large quantities of data — all of which must be handled securely.
- The Digital Government Strategy, issued in May 2012, became the latest in a line of federal initiatives aimed at harnessing technology so citizens and government workers can securely access data and services from any device.
- States are developing health insurance exchanges as part of the Affordable Care Act, which will require CIOs and CISOs to work with Health and Human Services Department officials to ensure data and systems are secure and health information stays private. (Most major ACA provisions will be put into effect by January 1, 2014, with final full implementation scheduled for 2020.)
- Virtually every state, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation that requires notification of data security breaches that involve personally identifiable information.
- The Federal Information Security Amendments Act of 2013, which recently passed the House of Representatives, would update FISMA by requiring agencies to adopt continuous monitoring and other solutions to improve real-time security awareness. (The Congressional Budget Office estimates it will cost $620 million between 2014 and 2018 to implement.)

Making the Case for Security Investments

There is rarely a good time to argue for government agencies to invest more tax dollars in IT, especially during times of budget deficits and sequestration. However, investments in security now will be far cheaper than fixing breaches after the fact. Losing valuable data, in and of itself, is bad enough. But agencies cannot put an accurate price tag on the loss of public trust that accompanies highly publicized data breaches. A smaller investment up front can go a long way toward avoiding such a dire scenario.

Federal, state and local IT managers know well that government technology investments rarely keep pace with those of the private sector. Case in point: In pulling together its 2012 NASCIO cybersecurity study, Deloitte compared its state government survey results with a study it did for the financial services industry.

According to Deloitte, more than 60 percent of the financial services firms it surveyed for a 2012 study said their security budgets had gone up; among state governments in the same timeframe, that figure was only 14 percent. In general, according to the Deloitte–NASCIO study, 84 percent of CISOs surveyed said that lack of funding was a barrier to addressing cybersecurity.

At the federal level, it can be hard to gauge agencies' investments in IT security as a portion of overall IT spending. Recently, IDC Government Insights analyzed security budgets and identified possible sources of confusion.

In the firm's report, *Benchmarking FY12 U.S. Federal Government IT Security Spending by Agency*, researchers concluded that because security solutions are often part of a larger system installation, it can be hard to identify how much of the investment is devoted to securing data. (IDC Government Insights is preparing an updated analysis, due out the second half of 2013.)

That said, federal agencies spent $14.6 billion on IT security in fiscal 2012, up roughly 10 percent from fiscal 2011, according to the administration's annual FISMA report to Congress. Of the total spend, 9 percent went to security tools and risk management, down from 17.7 percent in 2011. (Agencies spent the bulk of the funds on personnel: 90 percent and 75.5 percent in 2012 and 2011, respectively.) The overall federal IT budget for 2012 was $79.4 billion.

So the question becomes, how exactly does an agency make the case for more IT security spending? The answer is risk assessment, monitoring and reporting.

No one can deny that government systems, like many enterprise IT systems, are constantly under attack. But without formally assessing the risk to all types of agency data and information resources, IT managers can't know if they have the proper levels of security in place.

Without continuously monitoring the security solutions they implement, they can't know if they're working. And without regularly reporting the status of their security solutions, the data breaches they prevent (or don't) and the constantly evolving attack vectors that IT security systems encounter, IT security teams can't make credible arguments for preventive IT security investment.

In short, government IT managers must bolster their business case for IT security investments. In its February 2013 report, the GAO wrote of security programs it had reviewed: "A convincing assessment of the specific risks and resources needed to mitigate them would help implementing parties allocate resources and investments according to priorities and constraints, track costs and performance, and shift existing investments and resources as needed to align with national priorities."

At the federal level, the administration, in consultation with the Homeland Security Department, Defense Department, National Institute of Standards and Technology (NIST) and the Office of Management and Budget, has made clear where its IT security investment priorities lie:

- Trusted Internet connections, including baseline capabilities for situational awareness and monitoring
- Continuous monitoring, to mitigate risk and provide real-time security status and remediation
- Strong authentication, particularly via Personal Identity Verification and Common Access cards, to support multifactor authentication and encryption capabilities as a means of securing access to systems and data

Each will require new and upgraded systems and programs to help protect data and realize a more secure government IT infrastructure.

Securing Devices

Perhaps the greatest security challenge facing government today is the proliferation of mobile devices. By their nature, notebooks, tablets and smartphones (when granted access to agency resources) redefine (or break down) the network perimeter. And not just once, but every time they're used to log in to government resources from a conference room, living room, coffeehouse or other location.

Not to mention, mobile devices present the risk of agency data literally walking out the door, whether it's surreptitiously downloaded to a device, innocently accessed with no intent of harm or saved to a device in full accordance with policy but accidently lost outside agency walls.

Significant gaps that could prevent effective use of mobile devices fall into five areas:

- Security and privacy
- User authentication
- Data encryption
- Application security testing and evaluation
- Device sanitization

NIST Special Publication 800-124 Revision 1, Guidelines for Managing and Securing Mobile Devices in the Enterprise, is one of several NIST publications devoted to securing government systems. It specifically describes MDM solutions as a means of securing the growing number of smartphones and tablets entering the government workplace. MDM encompasses a suite of tools for enforcing security policies on devices, whether they've been issued by the agency or are workers' personal devices allowed through a BYOD initiative.

MDM takes two basic forms: brand-specific, using tools provided by one platform vendor, and third-party solutions, which support a wider variety of device types. In an increasingly heterogeneous mobile environment (especially one that supports BYOD), a third-party solution provides the most flexibility.

MDM software helps agency IT departments accomplish three basic functions to secure mobile devices and the data they access: remote security configuration, remote locking and wiping, and application management.

Remote Security Configuration

This all-encompassing category allows IT departments to control the security of mobile devices over a wide area network or wireless LAN. From a central location, the IT staff can restrict the hardware and software a device can use, encrypt data on the device, require authentication on the device before it can access resources, restrict applications, monitor security settings to make sure they're up to agency policy, and more.

Remote Locking and Wiping

When a device is lost or stolen, or a staffer no longer works for an agency, MDM software allows the IT staff to issue commands that either lock a mobile device until the user is authenticated, or wipes the device clean of applications and data. Both measures have personal privacy implications in a BYOD setting, so it's important that the agency make clear its mobile security policy before inviting users to access services using their own devices.

Application Management

Mobile apps are easy to download, which is one reason device users love them. It's also a reason mobile malware is on the rise. Controlling agency-approved mobile apps, as well as third-party apps that may attempt to access data they shouldn't, is a critical piece of an MDM solution.

Mobile application management (MAM) is especially important to the growing number of government agencies embracing BYOD programs. Advanced MAM solutions offer "sandboxing." A virtual sandbox is a walled-off area on a user's mobile device where only agency apps and data reside. Nothing outside the sandbox can access what's inside, and vice versa.

Sandboxing can help drive adoption of an agency's mobile security policy — critical to a successful mobile computing program — because it establishes an isolated area on the device that the agency controls, without demanding control over the entire device.

MDM solutions can also help IT organizations control the distribution of approved apps to employees' devices. Just as the IT team can push needed software, patches and OS updates to LAN-connected systems, it can also use an MDM solution to do the same for untethered devices. IT staff can also limit the apps that workers can download to their devices.

BYOS: Build Your Own Store

What is the best way for a government agency to control the apps that workers download to their devices? Control the app store.

One of the attractions of mobile devices is the ability to load any number of different apps. But some apps include malware or access resources on a device that they don't need to access, such as network connections or GPS functions. Just like commercial online app stores, government agencies can set up their own storefronts and control the apps their workers use.

Over the past couple of years, many agencies, including the Marshals Service, Veterans Affairs Department and Defense Advanced Research Projects Agency, have launched plans to build their own app stores. The benefits are twofold: App stores provide workers a place from which to download both agency-specific apps and third-party apps that have been vetted and approved for use.

Those with BYOD programs must negotiate policies of proper app use: It's difficult to control what workers download to their personal devices, to say nothing of keeping tabs on the millions of available apps they have access to.

But organizations can direct mobile device users to these internal stores for approved apps while also offering access to useful, entertaining, secure apps as an added value. No one wants to download malware to their personal device, meaning workers will likely find the agency app store a valuable service.

Beyond MDM

In addition to MDM solutions, government IT departments should monitor several emerging endpoint security options, which would be facilitated by an enterprise MDM system.

As mobile devices grow more powerful and increasingly roam between cellular and wireless LAN connections, developers are coming up with host-based firewalls for smartphones and other mobile devices. It's been debated whether a smartphone needs its own firewall, the way an end-user system does, because cellular networks tend to operate sophisticated network firewalls to control access and keep out malware.

But when workers connect via wireless LANs (and even when they don't), it's not unlike traditional client-network communications. And with smartphones capable of holding much more data, there is a growing need for mobile host-based firewalls that actually run on the device and monitor inbound and outbound connections.

These solutions can also be set to trigger alerts and to block specified traffic from entering or leaving a device. Capabilities such as these give users and IT staff a detailed picture of mobile app behavior and in-depth information about data traffic. Requiring host-based firewall protection is recommended under BYOD programs.

In addition, mobile antivirus protection and web security are increasingly important. Both function similarly on smartphones and tablets as they do on desktops and notebooks. It should come as no surprise that as more users come to rely on mobile devices, security threats begin to resemble what IT teams have dealt with on desktop platforms for decades. Mobile antivirus solutions can keep out malware, while mobile web security can help foil phishing attacks and similar threats.

Securing Data in Transit and at Rest

Perhaps the most obvious sign that organizations of all types are more focused on protecting their data is the rise of a solution stack collectively known as data loss prevention. DLP encompasses many security capabilities, from data discovery and inspection to various levels of encryption. The goal is to keep data safe whether it's being accessed over a network or resting in storage. But it starts by understanding the data an agency maintains, shares and generates.

For starters, DLP tools include identification and classification capabilities. Before they can prevent data loss, agencies must know what data they have and how important it is. Rapid technological advances have made it possible to better protect data in real time. But it makes little sense to invest in highly secure data loss prevention for all of an agency's information when only a fraction of it is of high value.

During data identification (or discovery), DLP software scans and analyzes data throughout the agency — on clients, servers, databases and more. In addition to understanding what data resides where, DLP software can analyze who accesses it, how they access it and what they do with it.

As a side benefit, DLP software can find old or duplicate data that can be consolidated. Agencies will find it is easier to secure data when it's stored in fewer locations.

As part of this process, DLP software uses pattern matching to identify sensitive data as described by the agency. It can search for telltale signs, such as Social Security numbers, keywords or other bits of information that IT and security professionals specify as indicators of data that requires special protection.

The DLP tools can then flag that data as sensitive so that in the future, officials can be alerted when the data is accessed, altered or transmitted. The DLP tools can also allow a transaction or block it, depending on a variety of factors, including who is accessing the data.

With data identified and classified, DLP solutions offer a number of protections. At the network level, systems examine data moving through various network points such as routers, switches and wireless access points. With the information gleaned through discovery and classification, DLP appliances scan email attachments, FTP uploads, web traffic and other network communications for sensitive data.

When a DLP device identifies data movement that violates agency security policy, it can block the data, quarantine it or encrypt it on the fly.

In addition to network-based DLP, endpoint products should be factored into a data security plan. Endpoint DLP tools monitor data traffic and enforce policy on users desktops, notebooks and other devices.

Endpoint programs can prevent users from copying information to a USB flash drive or send an alert when it happens. Most can prevent users from sending, receiving or printing sensitive files, and many can even keep users from copying and pasting sensitive data into other files or into email messages.

Endpoint DLP solutions are often agent-based products that must be loaded onto the endpoint itself to scan files, folders and databases. They are often part of a larger suite that also includes endpoint encryption, host-based firewall and antivirus protection, and network access control (NAC).

Encryption

A comprehensive DLP solution integrates well with encryption and user authentication systems. For example, a DLP system can be configured so that when sensitive data is transmitted across the network, it automatically routes to an encryption gateway before delivery.

Encryption is a broad security endeavor, historically the purview of larger agencies or those with the most sensitive data. But with data growing in size and importance across government, encryption has begun to play a broader role in IT security.

In a nutshell, encryption employs algorithms to make data unreadable to anyone who does not have the key that makes it readable. For example, a virtual private network (VPN) uses encryption to create a secure tunnel over the Internet through which remote workers can access agency data.

For data at rest, encryption may be enforced on a per-file, per-folder or whole-disk basis. Whole-disk encryption affords the most protection. It commonly requires user authentication, particularly on desktops and notebooks, because the OS is also usually encrypted.

Agencies may also use virtual-disk encryption, which encrypts virtual containers of files and folders that then behave like hard drives. Once a user provides proper authentication, the container is mounted as a virtual disk, providing access.

For data in transit, there are many tools for encrypting information that work at various network levels, including the data link, network and application levels. Data-in-transit encryption can require software agents on devices (as with a VPN) or not (as with web-based Secure Sockets Layer encryption). Some may effect network performance more than others or require more sophisticated key management.

Agencies can enforce encryption policies using MDM, DLP and other enterprise solutions. It is worth noting, however, that as part of any comprehensive data security solution, encryption requires planning. For example, encrypting data in transit might complicate a DLP strategy because a network-based DLP scanner may not be able to analyze encrypted files for potentially sensitive data.

Authentication

Authentication lets users decrypt or encrypt data by requiring them to present the proper keys. Authentication also allows access to networked resources, systems, applications and more. Increasingly, adequate security for government systems and data calls for multifactor authentication.

Traditionally, multifactor authentication has been viewed as something people know (a password or personal identification number) combined with a second item, such as a biometric scan (fingerprint or iris), a token (a USB device or smartcard) or, in some cases, a mobile phone or even a gesture.

But as IT infrastructures evolve to encompass mobile devices, cloud services and other systems that challenge the notion of a network perimeter, authentication (by necessity) is evolving and growing in sophistication as well. Agencies therefore increasingly consider multifactor authentication a mix of something workers know (password), have (smartcard) and are (fingerprint).

Encryption in the Cloud

At a time of cloud-first IT initiatives across government, who is going to secure data when it rests within a cloud provider's infrastructure? Whether an agency explores private-, public- or hybrid-cloud computing solutions, encryption must play a central role.

Among other tools, agencies should consider:

- Encrypted VPNs for all communication between the agency and the cloud service
- Application encryption, where feasible, such as for cloud-based email
- Storage encryption, both for offsite data storage and data-related cloud apps, such as collaboration and file sharing

Cloud encryption isn't always a no-brainer. Certain applications require responsiveness that encryption may hinder. In those cases, agencies must hammer out effective service-level agreements with providers to protect their information, or look to programs such the Federal Risk and Authorization Management Program (FedRAMP) for government-vetted cloud services.

Securing the Network

Even as agencies broaden IT security to focus more intently on data, proper network defenses will continue to play a critical role in protecting important assets. When identifying areas for investment, agencies should focus on four areas:

- Continuous monitoring
- Intrusion detection and prevention systems (IDS and IPS, respectively)
- Network access control
- Wireless network security

Because cybercriminals have stepped up the rate and sophistication of attacks, it's not enough for agencies to assess their network security posture only periodically.

NIST Special Publications 800-37, Guide to Applying the Risk Management Framework to Federal Information Systems, and 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, lay out the most detailed guidance on moving to a continuous monitoring approach:

- Pull information from a variety of sources.
- Use open specifications, such as the Security Content Automation Protocol (SCAP).
- Offer interoperability with other products, such as help desk, inventory management, configuration management and incident-response solutions.
- Support compliance with applicable laws, directives, policies, regulations, standards and guidelines.
- Provide reporting with the ability to tailor output and drill down from high-level, aggregate metrics to system-level metrics.
- Allow for data consolidation into security information and event management (SIEM) tools and dashboard products.

Although continuous monitoring is a relatively new best practice, many of the automated security functions that feed into it are well established: vulnerability, patch, event, asset and configuration management, as well as malware detection and software assurance.

Intrusion detection and prevention systems, a family of network security systems that is sure to feed information into a continuous monitoring solution, are well-established network security technologies that have grown more important as cyberattacks have evolved and multiplied.

An IDS is usually a network appliance, often a sensor that can examine data packets without effecting network performance. The IDS can sound an alarm if it detects an attack, but it does little else. It must be deployed in conjunction with other remediation technologies.

An IPS also is a security appliance or sensor, but it is usually installed inline with network traffic. Agencies can load signature files and other information into an IPS so it knows what to look for as it inspects packets. An IPS can also take immediate action, such as blocking traffic, if it detects an attack.

Network Access Control

Increasingly, agencies must also add layers of network security to accommodate the growing legion of mobile devices that must access government resources. A NAC solution is one approach.

When a mobile device attempts to log in to a government network, NAC systems check its security and other settings, compare them to security policy and decide whether to allow access, deny it, allow limited access or quarantine the device until it's brought up to proper security configuration. This may be accomplished by a software patch or by simply activating client security software that may have been accidentally turned off.

A NAC solution can be agentless (run from the network) or agent-based (run on each device). Agents typically scan devices for security settings, OS and app patches, as well as antivirus and host-based firewall software. A NAC solution is especially critical for agencies that have BYOD programs.

CASE STUDY

STATETECH

How Agencies Guard Against Mobile Malware

Technology controls include awareness and mobile device management.

Guarding Against Malware

Find out how some agencies are addressing burgeoning malware threats:

CDWG.com/secureinvest2

In short, a NAC solution helps separate secure clients from nonsecure clients, based on the agency's security policies. With more devices requiring wireless access to agency resources, other methods may be required, particularly in BYOD situations. One way to secure a network while allowing a BYOD program is to completely separate the BYOD traffic, granting these users access to some but not all internal servers.

Such BYOD-specific networks are usually wireless, given that they support mobile devices. They may be composed of a separate network of wireless access points, often set up outside an agency's secure network perimeter, with a secure, wired link back to the organization's resources. Such a separate, wireless BYOD network requires the same security measures as other wireless network access.

But whether wireless or wired, the security goal is the same: Ensure that only authorized workers have access to an agency's valuable data.

The Value of a Network Security Assessment

Third-party assessments are important for reviewing an IT system's security and identifying assets that may be at risk. No in-depth assessment can conclude that a system is 100 percent secure, but it can pinpoint weaknesses that could be exploited.

A comprehensive assessment offers a depth of analysis that simple vulnerability scanning or penetration testing do not. This is because it takes into account an agency's particular policies and risk posture – in other words, the human side of IT security, or what agency officials expect from their security systems. From there, an assessor tries to identify security issues that traditional tools, such as vulnerability scanners, cannot.

Why might your agency contract for a comprehensive, third-party security assessment? Because it's really three assessments in one:

- **Baseline assessment:** This will reveal how security systems currently operate in the environment and support agency policies.
- **Compliance assessment:** It will ensure that security systems meet applicable standards for government information security.
- **Progress assessment:** This review will evaluate how well the security measures taken meet the anticipated goals.

CDW Threat Check is one way to assess network security. With CDW Threat Check, an organization receives a monitoring appliance that automatically analyzes network traffic for threats and provides actionable insights.

The outcome of a comprehensive assessment is a detailed report that can serve to help agency IT professionals justify fresh investments in security. The report educates the IT department about issues not previously known nor understood, offers justification for investing in remediation, and explains the risks, should measures not be taken to secure systems against changing threats.

In today's budgetary climate, such a comprehensive assessment report could mean the difference between a data breach and an uneventful day in IT.

SHARE THIS WHITE PAPER

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW·G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.
All other trademarks and registered trademarks are the sole property of their respective owners.
Together we strive for perfection. ISO 9001:2000 certified
122211 – 130711 –

CDW·G® PEOPLE WHO GET IT™