CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

CYBERSECURITY AND SHADOW IT CHEAT SHEET

① Shadow IT

A term that describes employees using mobile apps and personal devices without the approval or knowledge of the IT department. This trend has become increasingly prevalent in recent years, due mainly to the rise of cloud computing and BYOD. Today's employees no longer need the IT department to install and enable new technology for them. They can open accounts on cloud services, use personal accounts, or download apps to their personal devices and immediately begin working with corporate data and sensitive content. Based on Cisco Cloud Consumption engagements, large enterprises on average use over 1,200 cloud services – and over 98% of them are Shadow IT.

② Differing Views

Some argue increase in flexibility outweighs the potential risk of using un-vetted online services, and that revenues and that revenues and productivity will rise as a result. It is often the source of most IT innovation and spending efficiency. Others say not so fast, these services are often:

- A duplication or waste of resources
- A source of security risks
- A way to unintentionally torpedo regulatory compliance efforts

③ Be Proactive

You must share with end users the concerns that IT has about Shadow IT.

- Identifying genuine threats
- Describing ways to avoid them
- What online behavior will and won't be tolerated

④ Understand the Problem

What services are employees, business departments using
What category do each of these services fall into (file sharing, productivity, social media or collaboration)
What are the risks for each services currently in use
What services are popular with employees and department management and should be evaluated for possible use on a full company basis
Are my firewalls and proxies effective at identifying and enforcing cloud use policies

Continue reading on next page >

CYBERSECURITY AND SHADOW IT CHEAT SHEET

(CONTINUED)

⑤ Engage with the Users

Identify areas of opportunity to optimize the experience of your employees as well as their workload..

Communicate IT's concerns, listen to what your users need from IT, and create the middle ground where none currently exists.

Find out why aren't employees coming to IT with their requests?

Is there too much red tape in the approval/fulfillment process.

Is there pressure to be all-productive due to increased global competition

Is there the need to be agile to survive

⑥ CISO's Role

The CISO also needs to be involved in managing shadow IT.

CISOs must put an end to draconian policies that restrict behaviors such as the use of mobile devices, cloud apps and new software tools.

They need to allow the business to adopt new technologies, especially those that improve productivity and efficiency while lowering costs.

By instituting this policy you can address security gaps created by new shadow projects while allowing employees to find innovative ways to do their jobs more effectively.

Provide Self Service Options ⑦

This can eliminate bottlenecks for IT department.

Do we have redundant services that employees are using

Are the services we offering inhibiting collaboration

Are employees or departments introducing additional cost by their use of these services

Speed and Efficiency ⑧

Employees who are keen to keep working with the best tools possible are often unaware of how their actions jeopardize the security of the company.

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

Continue reading on next page >

CYBERSECURITY AND SHADOW IT CHEAT SHEET

⑨ Prioritize Compliance

Shadow IT is a very serious and growing threat to IT compliance and cyber security, and most organizations have no idea how common it really is.

One of the big problems with compliance is that many people are lulled into a sense of security once a business has passed and been declared compliant. Rather than simply focusing on "becoming compliant" or being declared compliant, businesses should instead focus on managing compliance.

Much like your work with security and vulnerabilities is never through, so too is compliance work never truly finished.

Since compliance is not security, you should also be using vulnerability management to help your business stay secure. If you do, then compliance will almost naturally follow.

Staying on top of your security not only helps your business stay secure; it also helps you remain compliant!

Make sure IT has oversight over all corporate networks, devices and data with a formal response plan if a security incident occurs.

Employ technologies that include automated alerts and remote capabilities for neutralizing threats

- How do I quantify the risk from the use of cloud services and compare it to peers in my industry
- What services in house use sensitive or confidential data?
- What are the security capabilities of the services storing sensitive data?
- Which partners' cloud services are employees accessing
- What's the risk of these partners?

(CONTINUED)

⑩ Follow Best Practices

Change Your Attitude. Companies need to acknowledge that shadow IT could be harmful for their security and budget but it doesn't mean that companies should focus exclusively only on its negative effects. There are some positive benefits:

- Encouraging research of better apps
- Boosts productivity and business agility
- Offers flexibility and quick solutions for business needs

Analyze Your SaaS Apps. Organizations should analyze all SaaS applications and categorize them, as follows:

- Allowed - SaaS applications allowed by your IT department for general employee use.
- Restricted - unwanted and blacklisted for organizational use.
- Shared - utilized by entire company to increase productivity.
- Experimental - used by your employees but monitored during use for research.

Enlist Other Departments. Consult with them and get their support to manage IT even more effectively.

- Security - ensure security of application.
- Finance - Reduce overspending on software.
- Compliance - ensures company compliance with regulations and licensing restrictions.

Continue reading on next page >

CYBERSECURITY AND SHADOW IT CHEAT SHEET

CRAIG PETERSØN.COM

(CONTINUED)

11 Ensure Awareness Through Training

A good training program can only be effective when they advance knowledge and understanding of the topic and must address people's real life reactions to situations. That means learning not only what they have memorized but additionally how they would act/react to a given situation. These types of evaluations not only indicate where vulnerabilities lie, but also engage your employees in new ways that make security more realistic. With a baseline of employee knowledge established, you now can target the areas where your organization needs information security strengthening. creating content focused on your organization's needs. One of the best ways to engage employees is to keep the training concise and focused. Presenting information in interactive ways can be more time intensive, however, the investment is worth it for something this important. Engaging employees in security awareness means more than once a year training. Security needs to become a habit about which people no longer think but do reflexively.

Provide an Amnesty Period 12

Once you've dealt with the immediate dangers and know what's going on give everyone the chance to stop using the unapproved shadow IT applications. Give them a week or two to alert you why certain applications are necessary and you can then manage the exceptions. After the week is up shut everything unapproved down.

Continuous Management 13

Once you've dealt with the immediate dangers and know what's going on give everyone the chance to stop using the unapproved shadow IT applications. Give them a week or two to alert you why certain applications are necessary and you can then manage the exceptions. After the week is up shut everything unapproved down.

CRAIG PETERSØN
AMERICA'S LEADING SECURITY COACH