BSidesTO Talk Outline

* How it began
* Simpler times, simpler rules
* Then there came Mobile. That changed everything. Everyone wanted it
* Hello Gen Mobile
* What did people do to get what they wanted? BYOD
* How the IoT feeds the voracious appetite of BYOD
* Which brings us to the real problem: the human problem
* Mordor of Security
* The Culture of Indifference
* Can't regulate people or devices
* Growing so fast
* Why BYOD is a problem and how it affects Shadow IT/Data
* How Apple devices lack proper security
* The consequences and risks of BYOD. legalities
* It's not just the stuff, it's the attitude. Entitlement
* Access and Privileged Identitiy Mgmt. We aren't controlling what we can and need to control.
* We cave and comply.
* Privilege loses its meaning
* What hackers want – that privileged user account.
* Maintaining security on other people's devices
* Patch programs are hard enough. Good luck enforcing on other people's stuff
* How can you secure what you don't know
* Data Storage
* Privacy
* Liability issues
* Safe Harbour
* Data Localisation
* Data leakage
* Unauthorized data departure
* Shadow Data
* The Cloud and Shadow IT
* No recognition of barriers or boundaries. No respect for existing security principles
* Erika Chikowski. Insider threat and Shadow IT = focus on cloud security
* Where the tension occurs. We need to build a bridge to meet business needs and pull them out of the shadow
* Gartner predictions and the cases driving Shadow IT
* Shadow IT isn't going away. It's become how work gets done. We need to understand why to work with it so it doesn't work against us. Get policies that users will actually agree to
* The Culture of Indifference
* Thoughts by BOX owner. His new enlightenment
* Citizen dev platforms
* Cloud access Free-for-All
* Cloud services "how many are there"
* The real costs of using Cloud Services without control
* Cloud Security Challenges
* Shodan Demo
* What we can find and don't want to is out there, everywhere.
* Open and vulnerable
* How to regulate a device-driven society
* Genie is out of the bottle. Can't go back
* Old way – rule of least privilege can't be done the same way
* The stuff we know we have to do well we have to do even better: training & awareness; monitoring and inventory; securing hi-valu assets
* We need to up our game
* Getting our head in the Cloud.
* What's getting used.
* How to find out and monitor
* We need to ask WHY
* Keep your friends close bit. Meet them halfway
* Need to engage the support of the CSuites
* CASB – cloud access security brokers
* Utilize a hybrid cloud strategy
* If we want to change the outcome, we have to change the game

DETAIL:

Hi Everyone! Welcome! I’m Cheryl Biswas and my talk today is What Lurks in the Shadow? Addressing the Growing Security Risk of Shadow IT & Shadow Data.

So, here's the obligatory bit about me. I work with JIG Technologies here in Toronto where I do research, analysis & writing. I've loved tech since I watched Star Trek as a kid. You could say I've been a hacker at heart since I taught myself how to use computers and took them apart. I discovered InfoSec about a year and a half ago, and never want to leave. This presentation, and the opinions in it, are my own.

There was a time when the security lords ruled. Mere mortals only had whatever devices and access they were issued. Companies had “standards”. Remember those? You wanted a better, faster printer – it had to exist on the approved equipment list. You wanted the latest version of WordPerfect? Only if the company was ready to roll it out. But decisions took time. And you didn’t always get the answer you wanted.

It was easier to regulate things back then, when there were fewer things. Mobility wasn’t an issue because it wasn’t even a consideration. The available tech was enough to get the job done. But that’s the thing. Tech is always evolving, to meet the demands for faster, better, more. And how do you do more better and faster? One word. Anyone?

Mobile. Because the internet had become this happenin' place. Now, you could work anywhere, anytime.

Access all the data you want when you want it. But only with the newest, fastest devices. And were those on the approved standards list? Anyone?

No. Regulating tech was getting in the way of getting stuff done. Security became an inconvenience.

So what did people do to get what they wanted.

BYoD.

Everyone brings anything into work and plugs. It. In.

Be afraid. Be very afraid. Because we can’t see all the stuff, all the time.

So what do you do? Accept it? Regulate it? Or ban it?

According to Pwnie Express: “74% of companies are adopting BYOD policies. They need visibility into all devices on or around their networks.”

Because “the reality is that employees can and will often bypass your policy, sometimes by accident and sometimes on purpose.”

Which is bad because now there’s the … Internet of Things.

Yet even more stuff that plugs in.

And who uses all this stuff?

People. Unpredictable. Illogical.

And they are the constant variable in a security equation we just cannot seem to solve.

They are the unknown quantity.

Which for InfoSec, creates a very real fear of the unknown. CLICK

What do they do with those devices, what do they do with all that data…

How do we control what we don’t know?

CLICK Welcome to the *Mordor* of Security.

CLICK Where the eye of [BYOD](http://www.tripwire.com/state-of-security/latest-security-news/majority-of-organizations-have-no-byod-policies-2/) reigns supreme .

Easy-to-use devices are everywhere, creating an unprecedented level of end user entitlement.

And a little knowledge has become a very dangerous thing by letting people “help themselves” to data and network access.

So, what happens when users or employees take it upon themselves to decide what tech they want to use and how they want to implement it?

CLICK Shadow IT and Shadow Data.

Here’s the deal:

CLICK As the IoT proliferates, and human nature takes its course, we cannot out-engineer human failings and susceptibility.

So that device - and the freedom to use it as the user sees fit - override anything we currently put in place.

Then there are the tech-savvy staff who know how to do it for themselves and operate under their own autonomy, sought out as the rogue IT department.

Because who needs guidelines when you have Google?

CLICK And in the world of Shadow Data/Shadow IT

CLICK rules are known but not observed

CLICK risks are taken regardless of known consequences

CLICK and “keep it secret” definitely does not keep IT safe.

We’ve got a problem, and it’s more than just devices**…**

In our corporate realm, we have regular users and superusers. And for good reason. We need privileges in order to do certain things and we need privilege hierarchies to establish the right levels of access.

Here’s the problem: CLICK

“With great power comes great responsibility”.

And so, with higher levels of privilege come higher levels of risk.

The problem is that what we’re seeing happen in organizations and companies is a less discriminating assignment of privilege.

Per Erika Chikowski, while 92 percent of organizations in the US have some user monitoring in place only 56 percent are handling privileged identity management. Almost a third of those companies do not have someone actually analyzing or auditing how and when employees and contractors have privileged access to systems on even a weekly basis.

How many of you do regular password updates?Try 58 percent of US organizations.

Now, what percentage of US IT decision-makers share access credentials with other employees? Identity mgmt firm Centrify found nearly 60 percent

And from 200 of these decision-makers, they found that 52 percent of US-based IT employees also shared credentials with contractors.

Erika Chikowski

We all know about this one.

But now this approach is extending down into the ranks of ordinary employees.

We have all these devices, and a pervasive BYOD culture, demanding access to the networks and the data, all that lovely “big data”.

Oh the pressure.

And so we comply. We keep opening doors that should just. Stay. Closed.

As this culture grows, so does the sense of entitlement, spreading like a shadow across organizations.

For businesses it’s as a cost-saving measure, and a major convenience.

But businesses need to heed this warning:

When you agree to BYOD policies you put employees in the security chain. ZdNet

Privilege loses its meaning when that account status is being freely handed out. Cutbacks and reductions mean fewer guardians at the gate in IT. Under pressure to keep things running, meet demands, we resort to the path of least resistance to “simplifying the process.” Why not enable users to resolve some of their own problems by raising their status? Let marketing have access to all the data – it’s just reports. Let people update corporate social media accounts – there’s nothing to worry about there.

But we know there is. All a hacker needs is that one key word to get in. Once in, they can find their way up through the labyrinth of security like a rat through a series of tunnels.

Remember Cyber-Caliphate – when they hacked US Military social media accounts this winter?

Those accounts with elevated privilege are prized by hackers.

Per the 2015 Data Breach Investigations Report by Verizon:

“these passwords are worth their weight in gold, and have root, admin, and read/write access for critical infrastructure, data and applications.” <http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/>

It’s one thing to try and keep all your corporate devices patched and up to date. Try enforcing that on individuals.

We know what happens when security patches aren’t updated: how hackers exploit those vulnerabilities in Adobe, Internet Explorer, WordPress.

What happens when individuals operate as individuals, and make independent decisions about data storage and transmission?

Alien Vault shows the risk of likelihood in this threat matrix. The biggest circle: Shadow IT. It’s about intent, frustrated users jumping the barriers we put in place for their own security, and then risking everyone’s security. Internal employees and contractors set up their own wireless LAN access points. Using personal technology for business functions, with no formal BYOD policy. Sending sensitive, confidential information across open, unsecured channels without regard for compliance or regulations. Rogue users of cloud services. What do you do when your greatest security threat comes from within?

Who are #GenMobile . According to Aruba, and others, they are:

the mobile workforce we now have

they are part of the enterprise realm

a flexible, transparent and collaborative presence in your workforce”

and …

“for the security of company data and IT systems,   
there may be cause for concern.”

Question: what percentage of workers do you think will go ahead and do self-service IT?

Aruba Survey says 77%

Hello Shadow.

And businesses just aren’t ready. They didn’t see this coming, so they didn’t put provisions in place. Stats show over 37% didn’t have a mobile security policy in place. As for enforcing things like password protection on corporate mobile devices, almost 1/5 of workers don’t do that. <http://news.arubanetworks.com/press-release/enterprise-security-threat-level-directly-linked-user-demographics-industry-and-geogra?_ga=1.13247991.1901946379.1433264944>

We are battling a culture of indifference.

Side-stepping company policy in favour of expediency happens everywhere, every day because it’s easier to just download a the software program online rather than go through the approval process.

A recent study by Aruba Networks surveyed 11,500 workers across 23 countries. Hands up if these are part of your daily fight:

And they caution:

**“Businesses are ill prepared for the high-risk, high-growth mindset of the** [**#GenMobile**](http://cts.businesswire.com/ct/CT?id=smartlink&url=http://www.arubanetworks.com/pdf/solutions/GenMobile_Report.pdf&esheet=51077933&newsitemid=20150414005111&lan=en-US&anchor=) **workforce”**

If you haven’t heard of it, this website shows all things connected to the internet in real time. You can do a variety of searches. By device, country, company. OR Password.

What happens when we enter “default”?

Whoa. That’s a lot of devices out there, all sitting wide open

What happens if we modify the search a little. See how Brooklyn tops the list?

Then we zoom in on Brooklyn, right there, and find out even more stuff we shouldn’t know.

Yes. It’s ***that*** bad.

How do we regulate a society that is essentially device-driven?

It isn’t just the servers and desktops at the office… everywhere we go, anything we touch – we’re connected. Fitbits, Apple watches, tablets, flash drives, smartphones – this ability to portably “plug in,” and then help ourselves is one we don’t understand and we’ve lost any control over it we had. Current rules can’t apply when the game itself has changed. Clearly, what was working isn’t working now. Just say “no”? If only it were that easy.

Maybe it’s a matter of regaining control.

Can we get corporations to adopt and enforce the Rule of Least Privilege? The original concept originated 40 years ago.

You can reference the paper back to SANS 2003 here. <http://www.sans.org/reading-room/whitepapers/bestprac/implementing-privilege-enterprise-1188>.

The reality is it’s a hard concept to sell. And that’s before you let the genie out of the bottle. So, are you going to be the one to claw back access, and restrict devices?

Training and awareness are a given. If we do it regularly, not just reactively, it will pay off. Because Knowledge is power. It can help us create the culture we need to forge security out of insecurity.

Then there are inventory and monitoring. These are Musts. Current and complete inventories are essential to your first line of defense as per SANS .

And what are the high-value assets we need to secure most?

But this is about what we’re not capturing. If we’re really going to catch stuff in time, we need to be tracking all the people and all their devices all the time.

We can keep asking nicely, but when that doesn’t work …

We need to get our head in the cloud.

How many of you are having issues with cloud access free for all where you work?

Cloud apps are info pipelines for users, and external storage dumps for corporate data. We need to understand what is the user trend, how are cloud apps working, what is duplicated.

There are some new products that address this.

Netskope came out late 2013. If you want to know who’s been sending what up into the cloud, Netskope lets you do that. It’s about helping CIOs see ”the inner workings of external cloud apps”, or Cloud Application Analytics & Security. Netskope CEO Sanjay Beri says this: As workers demand more effective tools to do their jobs, it’s inevitable more cloud apps will be introduced to the enterprise without IT’s knowledge. Out vision is to help CIOs tackle the accelerating shadow IT conundrum with detailed realtime insights”

And if it’s become an all-access pass to apps, Skyfence claims it can help you rein that in. It’s designed to help you enforce data leakage policy. It uses all the right buzz words. Visibility. Compliance. Shadow. And it’s all about taking back control.

And then there’s this.

“Keep your friends close, but your enemies closer. “

This may sound radical, but what if we find the ways to work together with the folks who sidestep the rules. Meet them halfway and say “yes” sometimes when they are used to hearing “no” all the time. A little cooperation leads to a little collaboration leads to information we need.

I know. Crazy talk. But there are experienced voices advocating this as the new path through some treacherous lands.

Yes. There are things we can do. We get security, but we cannot realistically expect most of the world to be where we are. We can do more to understand the actual needs of the businesses we’re working to secure. There’s a lot of talk out there about taking this to the suites. The C Suites. We know they stop listening when we deliver our warnings and lectures. While we both need to keep things secure, our priorities can seem mutually exclusive. They shut down when we impose our restrictions on their requirements. What we keep doing just isn’t working.

So what if we get a better handle on what people really need and want? What if we help them understand security is a strategic partner now more than ever, and not the pain in the ass they think? Breaches cost bucks, big-time. That directly impacts profit and bottom-line. I’m not promising we can prevent breaches. But we can shift gears, take our cues from the rapid developments of Cloud, Everything as a service, and Big Data. It’s a different terrain, but we’ve still got to run it faster, better than the guys who are out there waiting, counting on what our end users will do and won’t follow.

Because there is no one ring, no fires of Mordor, that will create the culture we need to forge security out of insecurity.

If we're going to change the outcome, we have to change the game.

I’d like to give a huge thank you to BSidesLV for Proving Ground and a terrific con. And to my mentor, Phil Young, who was fantastic. Those are my contact deets. And one request before you go:

Could you all lift you bottles and join me in a toast to a good friend who can’t be here this week: You probably know him as da\_667. So everyone:

Ayyy LMAO