




What Lurks in the Shadow

**Addressing the Growing Security
Risk of Shadow IT & Shadow Data**

By @3ncr1pt3d

Cheryl Biswas

-  JIG Technologies
@JIGTechnologies
- **Works for: JIG Technologies**
- **Does what exactly: security researcher, analyst, writer of things**
- **Trekkie, techie, maker, baker**
- **Bridging the gap between tech and non-tech**

Necessary Disclaimer: All content is my own and does not reflect the opinions of my employer



Security Lords

16/11/2015

BSidesTO: What Lurks In The Shadow by
@3ncr1pt3d



Faster. Better. More. Tech.



#GenMobile

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

<http://www.arubanetworks.com/mobileriskindex/>



An illustration featuring several hands holding up various mobile devices including smartphones, tablets, a laptop, and a flip phone. The devices' screens display Wi-Fi symbols. The background is filled with numerous blue icons representing different digital concepts such as social media, communication, and technology. The text 'BYoD' is prominently displayed in the center-right.

BYoD

A man in a red shirt is smiling and holding a tablet displaying a smart home interface and a small IoT device. He is standing in a backyard filled with various smart home appliances and IoT devices, including a smart refrigerator, a smart oven, a smart washing machine, and a smart dryer. The backyard is also decorated with string lights and a small table with a lamp. The scene is set at dusk, with the house's interior lights visible through the windows. The text "Internet of So. Many. Things" is overlaid on the top of the image.

Internet of So. Many. Things

16/11/2015

BSidesTO: What Lurks In The Shadow by @3ncr1pt3d

8

16/11/2015

BSidesTO: What Lurks In The Shadow by
@3ncr1pt3d

The Human Factor

A still from 'The Lord of the Rings: The Two Towers' showing the four Hobbit characters from the Baggins family standing in a crowd. From left to right: Legolas (wearing a brown vest), Gimli (wearing a dark red vest), Aragorn (wearing a light green vest), and Arwen (wearing a dark green vest). They are all looking forward with serious expressions. The background is a dense crowd of people, some wearing armor.

Fear of the Unknown



The Dark World

Shadow IT/Shadow Data

In the Land of Mordor

Where the Shadows Lie

Keep it secret, keep IT safe



IT'S MY PRECIOUS

MINE, MINE!

16/11/2015

BSidestO: What Lurks In The Shadow by
@3ncr1pt3d

12
memegenerator.es

“Employees in every cubicle are using Box, Workday and Salesforce, and they’re not waiting for IT’s permission to do so. They’re using their own apps on their own devices. Many are spinning up servers in the cloud for infrastructure in the cloud, a practice dubbed bring your own server. So privilege is now being consumerized like apps and devices.”

- Forbes

“When you agree to BYOD policies, you put employees within the security chain”.

- ZDNET



Bad Apples

Pass on the Passwords

- 51% Single password/numerical PIN
- 58% NO policies of software to enforce better passwords
- 56% Shared passwords
- 17% Used company-provided password mgr
- 60% Accessed confidential corporate data





Unprotected and Connected

- **questionable WiFi networks via the local coffee shop hotspot**
- **unapproved cloud storage**
- **really, really bad USB**

UPDATE ADOBE FLASH PLAYER?

AIN'T NO BODY GOT TIME FOR DAT

Unpatched Software

- Windows and MacOS
- Applications (PDF, Office)
- Mobile phones, tablets
- Web Servers (Heartbleed)
- Others (Java)



Security

means never
having to say
you're sorry

Data Security Tools In The CIO's Toolbox



Encryption



Access Policies



Tokenization



Data Masking



Security Intelligence

Cyber Insurance



A culture of indifference.

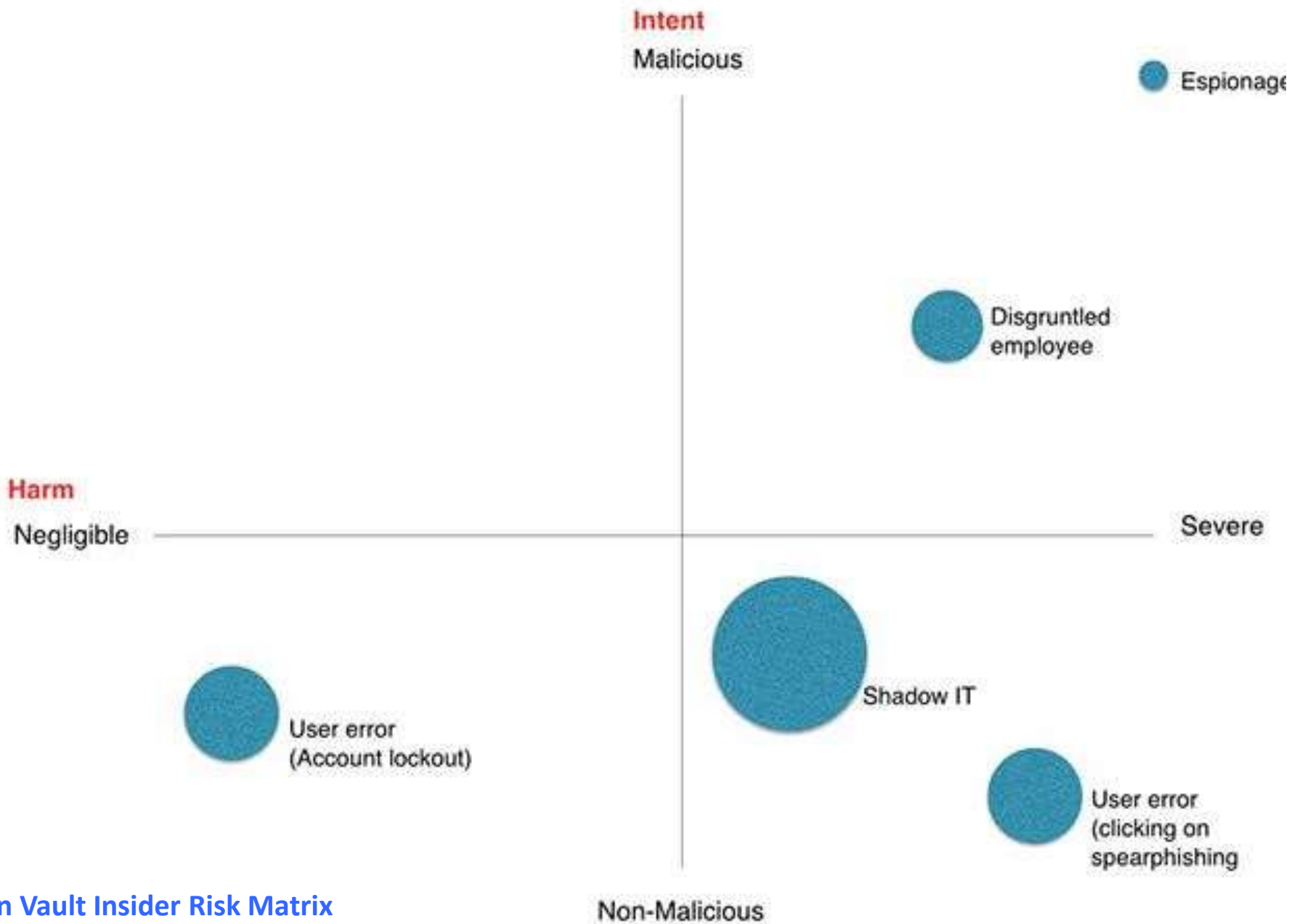
Sharing as the norm – devices, data, passwords

Indifference towards security – the assumption that security is somebody else's problem; not worried about their own responsibility

Self-empowerment succeeds over existing rules (Aruba Networks)

“Businesses are ill-prepared for the attitude of next generation employees who own mobile devices, and may be placed at risk as the BYOD trend causes fractures in security enforcement.”

- ZDNet



Alien Vault Insider Risk Matrix

**WITH GREAT POWER COMES GREAT
RESPONSIBILITY**

**“All identities are
not created equal”**

**With great power comes
great responsibility**

-ALBUS DUMBLEDORE

Great Power, Great Responsibility

- 92% orgs have user monitoring
 - 56% handle privileged identity mgmt.
 - 58% corps do regular password updates
 - 60% IT decision makers share creds
 - 52% share creds with contractors
- >20% analyze or audit privileged access

“IT departments often give non-technical executives (e.g. VP of Sales, CEOs, CFOs, etc.) broad privilege inside corporate applications, figuring it is better to give too much freedom to upper management than get yelled at when someone can’t create a report.”

- Forbes

“It is scary to think that this many people consider it normal for employees to have access to data that they shouldn’t have and for companies to not know where their missing data has gone.”

- David Gibson, VP at Varonis.

erCaliphate

The Loss of Privilege



Central Command

COM

Twitter for U.S. Central
Command (CENTCOM). *Follow/RT
= equal endorsement.

AFB, Tampa, FL

com.mil

March 2009

16/11/2015
Tweet to U.S. Central Com...

you isis

TWEETS
3,671

FOLLOWING
1,268

FOLLOWERS
109K

FAVORITES
30

Tweets

Tweets & replies

Photos & videos



U.S. Central Command @CENTCOM · 4m

AMERICAN SOLDIERS,
WE ARE COMING, WATCH YOUR BACK. ISIS.

#CyberCaliphate

13 1



U.S. Central Command retweeted

CJTF-OIR @CJTFOIR · Jan 7

BSidesTO: What Lurks In The Shadow by
@3ncr1pt3d



One Ring to rule them all.

The hearts of men are easily corrupted. And the ring of power has a will of its own...

Time
for
a little talk
about
B I G
Data

THE MOST DANGEROUS INSIDERS

ADMINISTER & MANAGE INFRASTRUCTURE

Privileged Users



59% RETAIL
63% FINANCIAL SERVICES

Privileged Users include System Administrators, Network Administrators, Linux/Unix Root Users, Domain Administrators and other IT roles.

Partners with Internal Access



51% RETAIL
43% FINANCIAL SERVICES

Contractors/Service Provider Employees

(Snowden was a contractor)



45% RETAIL
40% FINANCIAL SERVICES

Who Touched the Data?

“It’s not good enough to merely resist the rise of BYOD, if people can still access corporate e-mail when they get home...”

John McAfee



Source: GTB Technologies

I seek what you leak.



DATA LEAKAGE

**Ensure sensitive information on laptops,
mobiles and removable media is encrypted.**

**Check email recipients before sending and be
mindful of information you post online.**





Data Transfer on the Rocks

No More Safe Harbor

**European Court of Justice
Rules Agreement is Invalid**



What's Mine is Mine & What's Yours is Mine Too

Sh*tposts from the Trenches

**Razz-Ma-Tazz**
@GRC_Ninja

Infected BYOD laptop, n+4hrs to find it in the network NOC has no perms to do L2 ACL mods, it's spewing shit out port 80, & WAP is UNK. FML

11:59pm - 27 Oct 2015 - TweetDeck

8 FAVORITES



Reply to @GRC_Ninja

**Munin** @munin **Lore Keeper** 14h
[@GRC_Ninja](#) Why doesn't the NOC have perms to nail the L2 ACL down?
[View](#)

**Munin** @munin **Lore Keeper** 14h
[@GRC_Ninja](#) 'cuz that seems a little bit of a problem.
[View](#)

**Razz-Ma-Tazz** @GRC_Ninja 13h
[@munin](#) I'm not in charge, I just work here....apparently only an NetEng can do that around here....but yeah we're almost n+5 and nada
[View](#)



Spoopy DA 667

@da_667

cyber security policy success is
having the authority to tell the
userbase no, and having that
decision stick

2:35pm - 5 Nov 2015 - TweetDeck



Spoopy DA 667

@da_667

[@3ncr1pt3d](#) BYOD in a nutshell:
Here's a bunch of security controls
that we want you to have on your
device in order to run e-mail/chat.

2:52pm - 5 Nov 2015 - TweetDeck

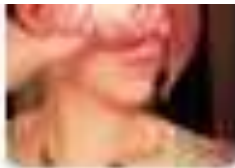


Spoopy DA 667

@da_667

BYOD is goddamn stupid. Device control suites often times don't do enough and are in morally and legally grey zones.

2:51pm · 5 Nov 2015 · TweetDeck



darth lsly
@lslybot

Telling users no, when it matters, to protect themselves and your company/network. [#abusepolicy](#)

Spoopy_DA_667 @da_667

cyber security policy success is having the authority to tell the userbase no, and having that decision stick

3:27pm 5 Nov 2015 Tweetbot for iOS

Let's do a little Demo

<https://www.shodan.io/>





Explore

Membership

Contact Us

Blog

Enterprise Access

Exploits

Maps

Download Results

Create Report

TOP COUNTRIES



TOP CITIES

Englewood	4,405
Ashburn	133
New York	109
Houston	26
Chicago	26

TOP SERVICES

Telnet	5,100
FTP	4,403
HTTP	14
9002	5
Elastic Search	4

TOP 16/11/2015

Showing results 1 - 10 of 10,291

184.159.114.202

CenturyLink

Added on 2015-07-02 18:28:58 GMT

United States

Details

[2J][H]

***** Important Banner Message *****

Enable and telnet **passwords** are configured to "**password**".
 HTTP and HTTPS **default** username is "admin" and **password** is "**password**".
 Please change them immediately.
 The switchport interfaces are enabled with an address of 10.10.10...

69.29.151.150

69-29-151-150.stat.centurytel.net

CenturyLink

Added on 2015-07-02 18:17:10 GMT

United States, Haleyville

Details

[2J][H]

***** Important Banner Message *****

Enable and Telnet **passwords** are configured to "**password**".
 HTTP and HTTPS **default** username is "admin" and **password** is "**password**".
 Please change them immediately.
 The switchport interfaces are enabled with an address of 10.10.10...

157.130.3.24

valueoptions-3.commer...

Verizon Business

Added on 2015-07-02 18:17:07 GMT

United States

[2J][H]

***** Important Banner Message *****

Enable and telnet **passwords** are configured to "**password**".

Country. Company. Device. Password

Default

BSidesTO: What Lurks In The Shadow by
 @3ncr1pt3d

TOP COUNTRIES



United States

550

TOP CITIES

Brooklyn	12
New York	7
Philadelphia	6
Woodstown	5
Washington	5

TOP ORGANIZATIONS

Verizon Business	550
------------------	-----

Showing results 1 - 10 of 550

157.130.53.214

valueoptions-gw.customer.alter.net

Verizon Business

Added on 2015-07-02 18:17:07 GMT

 United States[Details](#)

[2J]H

***** Important Banner Message *****


Enable and Telnet **passwords** are configured to "**password**".
HTTP and HTTPS **default** username is "admin" and **password** is "**password**".
Please change them immediately.

The ethernet 0/1 interface is enabled with an address of 10.10...

65.216.163.97

Verizon Business

Added on 2015-07-02 13:04:53 GMT

 United States, Salem[Details](#)

[2J]H

***** Important Banner Message *****


Enable and Telnet **passwords** are configured to "**password**".
HTTP and HTTPS **default** username is "admin" and **password** is "**password**".
Please change them immediately.

The ethernet 0/1 interface is enabled with an address of 10.10...

65.197.144.137

Verizon Business

Added on 2015-07-02 08:26:43 GMT

 United States

[2J]H

***** Important Banner Message *****



65.223.159.85

City	Brooklyn
Country	United States
Organization	Verizon Business
ISP	Verizon Business
Last Update	2015-06-30T14:48:28.540521
ASN	AS701

Ports

22

23

80

Services

22

SSH

SSH-2.0-RomSSHe11_4.31

Key type: ssh-dss

Key: AAAAB3NzaC1kc3MAAACBAKZf6qtRHGjPFP3drwO1m2814fpN5X5c8ArkeKhV3aTzY404uwCsSv



So Where Do We Go From Here?

“Just Say No.”

Current rules can't apply
when the game itself
has changed.
What was working
isn't working now

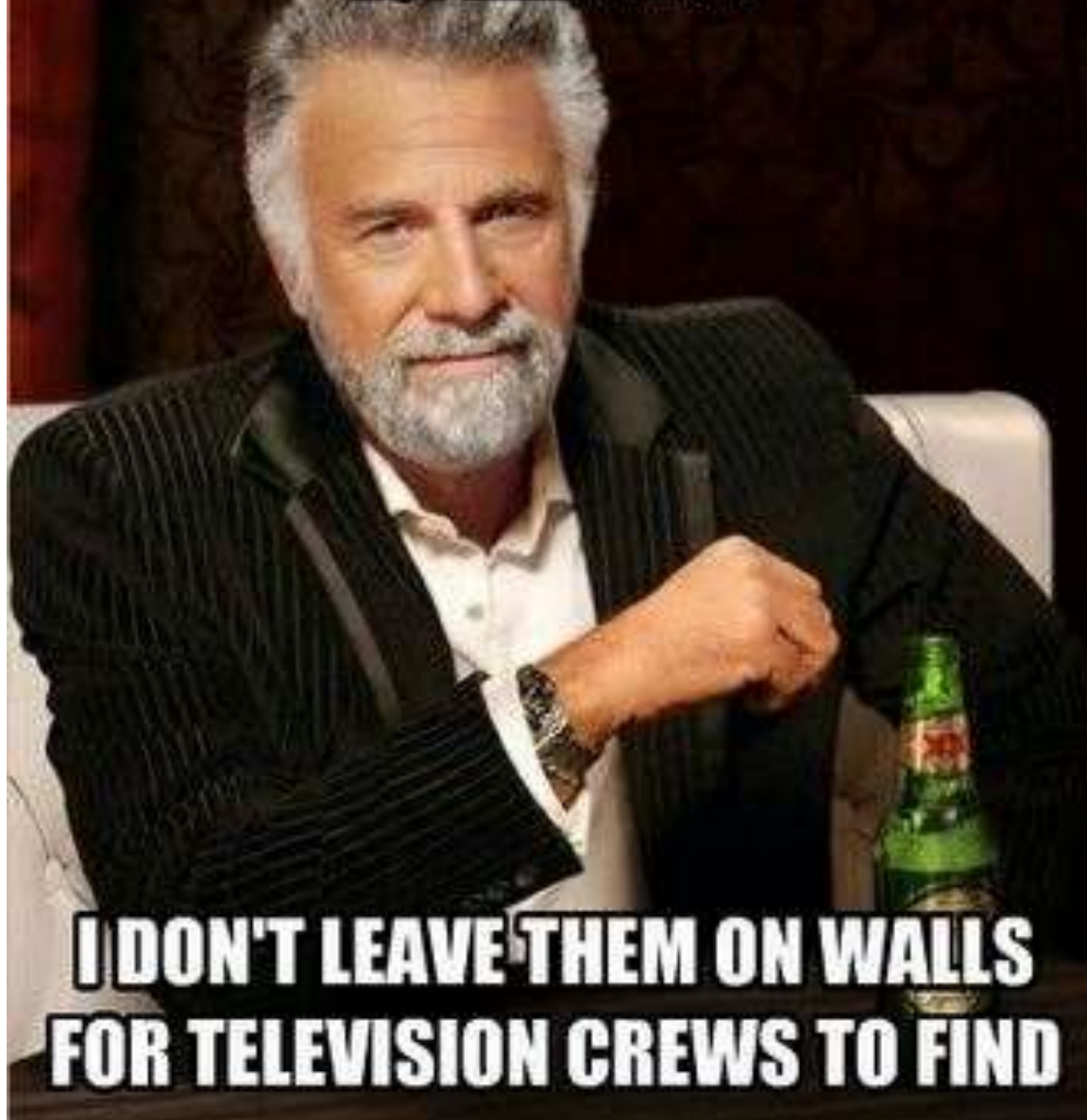
Least Privilege:

“Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily this principle limits the damage that can result from an accident or error.”

- SALTZER, J.H. and SCHROEDER, M.D.

**We've taken the lid off Pandora's box.
I don't think it ever goes back on.**

**I DON'T ALWAYS WRITE DOWN PASSWORDS,
BUT WHEN I DO...**



**I DON'T LEAVE THEM ON WALLS
FOR TELEVISION CREWS TO FIND**

What Are We Missing

- Training and Awareness
- Inventory and Monitoring
- Secure Hi-Value Assets
- ????

The Cloud



No Idea What They're Using, No Idea What They're Losing

- 15x more cloud services used to store critical data than CIOs authorized
- IT says 51 active cloud services. Survey says 730
- Use growing exponentially.
- 1000 external services per company by 2016

A person wearing an orange sweater is shown from the chest up. Instead of a head, there is a large, fluffy white cloud. The background is a bright blue sky with some lighter clouds. The text is overlaid on the upper part of the image.

30% of business critical info is in the cloud.

Most cloud apps are third party apps.

- Ponemon Institute



**Shadow IT
isn't
going
anywhere ...
Gartner says so**



- The last decade of the enterprise was defined by mass collaboration, the next decade will be defined by mass integration.
- IT should be the information enabler.
- If you're not the simplest solution, you're the target of one.
- History repeats itself in the technology industry. Pay attention to where customers are going.



@levie | BOX

AARON LEVIE
CO-FOUNDER & CEO

<http://aaronlevie.com/aaron-levie-coo-box/>








To Build a Better Mousetrap, Draw A Bigger Circle

The Way Forward

- Ask what users really need and want
- Show the CSuites why we are their strategic partner
- Shift gears and adapt
- Projections based on Cloud, Big Data, Everything as a Service



**As for that one ring
that rules them all ...**

**The World has
changed. And so must
we.**

Thank You So Much!

BSidesTO

Contact Deets: **@3ncr1pt3d**

ca.linkedin.com/in/cherylbiswas

<https://whitehatcheryl.wordpress.com/>

