



Securing your Digital World

Cyber Security for Small Business Enterprises

Sonny Hashmi

Managing Director, Global Public Sector, Box





The Small Business Technology Coalition

Box is proud to be a founding member of the "Small Business Technology Coalition" established by the US Small Business Administration (SBA), a partnership of private sector technology companies, committed to the success of small businesses across America.

We are excited to offer technology expertise and knowledge, as well as a starter set of tools to members of the small business community.

[List of Upcoming Events](https://www.sba.gov/techcoalition/events)

(<https://www.sba.gov/techcoalition/events>)



Cyber-security challenges are escalating



Cyber-security is a top priority for leaders



IMPVERVA Gartner Toolkit for CISOs: Prebuilt slides to share with the Board

Home > IT Strategy > CIO Role

NEWS ANALYSIS

State CIOs will focus on security and cloud in 2016



Credit: Thinkstock

MORE LIKE THIS

Bold CIOs are breaking free of legacy tech

Forecast 2016: Essential data points for the tech year ahead

State CIOs List Security as Top Priority for 2015

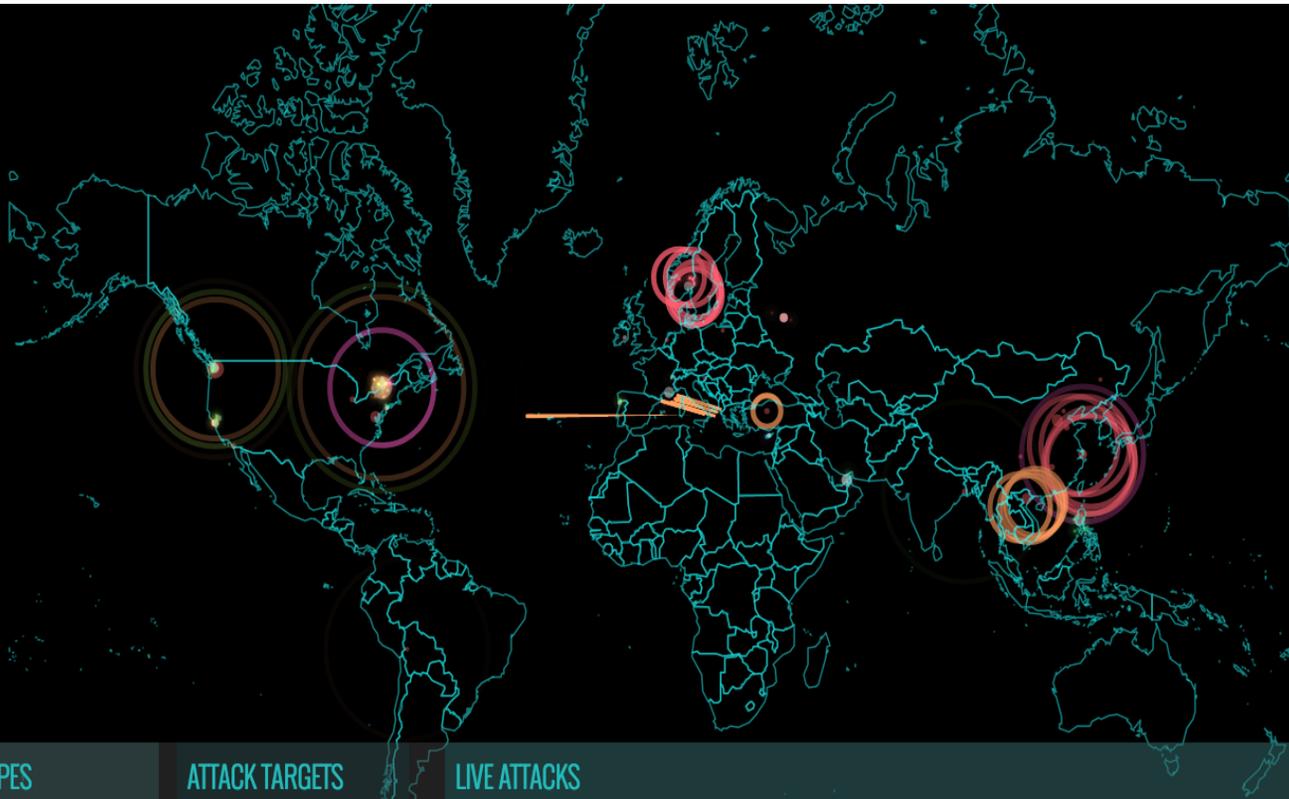
on IDG Answers How to turn on Windows 10's 'Find My Device' feature?



The State of SMB CYBERSECURITY IN 2015

A look ahead to SMBs' perceived challenges around cybersecurity, the cloud and planning for 2015

Primary research conducted by Spiceworks Voice of IT on behalf of CloudEntr. September, 2014



ATTACK ORIGINS

#	COUNTRY
40	United States
24	China
8	Vietnam
5	Russia
3	Turkey
2	India
1	Slovenia
1	Poland
1	Netherlands
1	Cyprus

ATTACK TYPES

#	PORT	SERVICE TYPE
31	25	smtp
13	23	telnet
10	53413	netis-router
5	1	tcpmux
5	1433	ms-sql-s
3	445	microsoft-ds
3	8080	http-alt
2	50856	xsan-file-system
2	3389	ms-wbt-server
2	465	igmpv3lite

ATTACK TARGETS

#	COUNTRY
48	United States
10	Philippines
9	United Arab Emirates
8	France
5	Russia
5	Norway
1	Portugal
1	Ireland
1	Cyprus

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
14-20-56.807	Vietnam Post And Telecom Corporation	14.162.143.153	Hanoi, VN	Aix-En-Provence...	telnet	23
14-20-56.807	Vietnam Post And Telecom Corporation	14.162.143.153	Hanoi, VN	Aix-En-Provence...	telnet	23
14-20-56.806	Vietnam Post And Telecom Corporation	14.162.143.153	Hanoi, VN	Aix-En-Provence...	telnet	23
14-20-56.806	Vietnam Post And Telecom Corporation	14.162.143.153	Hanoi, VN	Aix-En-Provence...	telnet	23
14-20-56.477	Chinanet-Zj Shaoxing Node Network	122.236.15.41	Hangzhou, CN	Oslo, NO	ms-sql-s	1433
14-20-56.476	Chinanet-Zj Shaoxing Node Network	122.236.15.41	Hangzhou, CN	Oslo, NO	ms-sql-s	1433
14-20-56.476	Chinanet-Zj Shaoxing Node Network	122.236.15.41	Hangzhou, CN	Oslo, NO	ms-sql-s	1433
14-20-56.476	Chinanet-Zj Shaoxing Node Network	122.236.15.41	Hangzhou, CN	Oslo, NO	ms-sql-s	1433
14-20-56.475	Chinanet-Zj Shaoxing Node Network	122.236.15.41	Hangzhou, CN	Oslo, NO	ms-sql-s	1433
14-20-55.959	Shanghai Qianwan Network Co. Ltd	219.235.1.84	Shanghai, CN	De Kalb Junction...	complex-link	5001



HOME

EXPLORE

WHY NORSE?



Some numbers to get you thinking...

- End users are perceived as the single weakest link in security infrastructure by **95%** of IT pros
- Security is considered more important (and therefore supercedes) than convenience in **63%** of organizations
- **54%** of security breaches caused by human error
- **\$3.8M** average cost of a data breach to a company's bottom line
- **43%** of teams and departments acknowledge using cloud services in companies that forbid cloud use (or have no plans to use cloud)
- Average company CIO acknowledges using **6-8** cloud services
- Average company actually uses **45-50** cloud services, some over **200!**

SpiceWorks voice of IT for SMB priorities

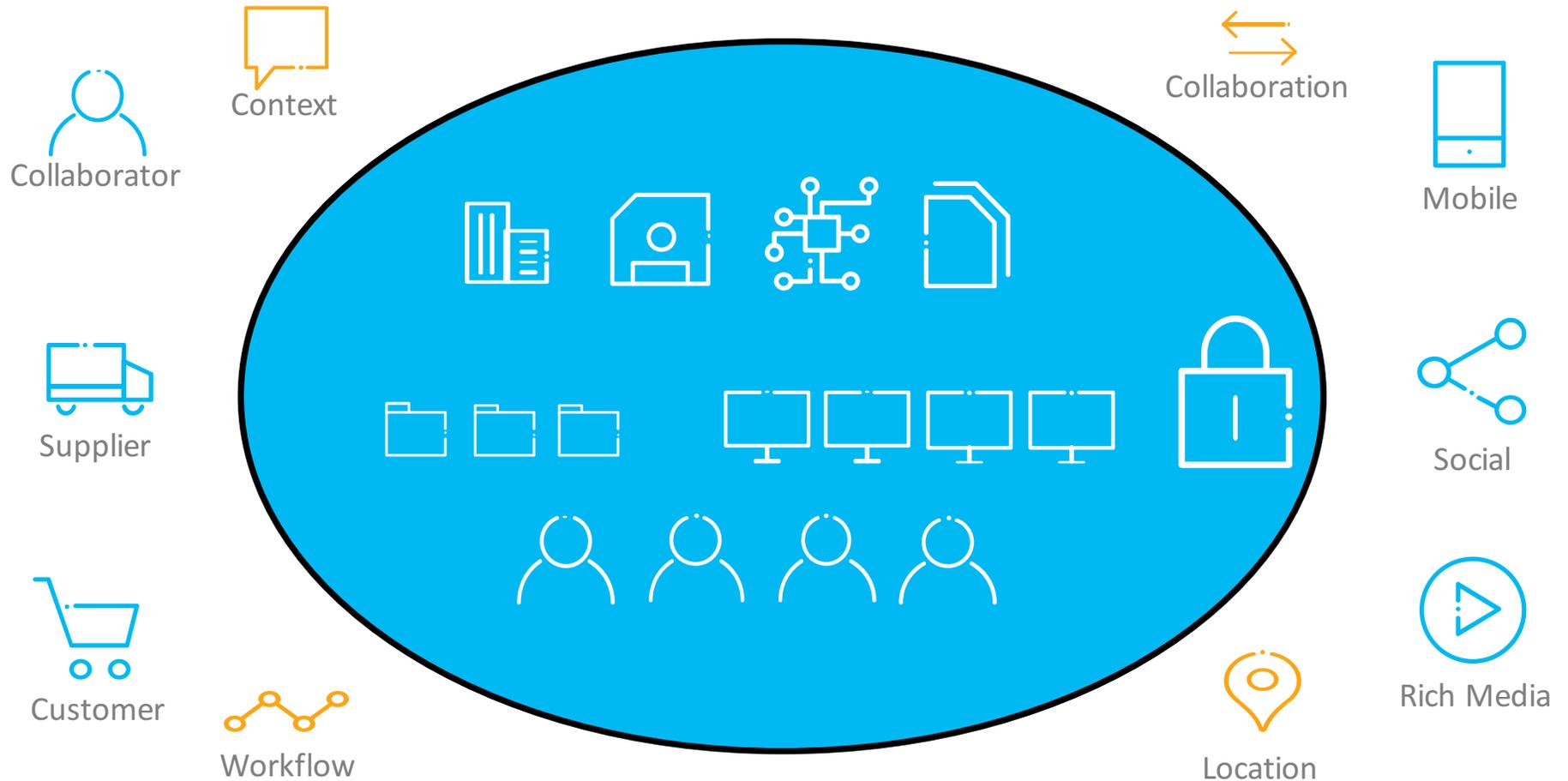




Cloud services are not the enemy

In fact, modern enterprise cloud solutions are generally much more secure than traditional/legacy IT systems

Traditional security model is not sufficient



Modern Enterprise Security Challenges

INSECURE COLLABORATION



Email attachments
FTP
Mailing CDs / USBs

58% of senior managers have sent sensitive information to the wrong person.

- CSO Magazine, Study by Stroz Friedberg

DATA PROLIFERATION



Duplication of files
Use of online apps

49 file sharing services are used on average in a single company.

- Skyhigh Networks study of 25 companies – Q1 2011 Cloud Adoption Report

INSECURE DEVICES



Stolen devices
Lost devices
Insecure back ups

4.3% of phones used by or issued to employees are lost or stolen annually.

- McAfee and Ponemon Study

HUMAN NATURE



Smart people / dumb actions
Organized Crime
State / Corporate Espionage

54% of security breaches are due to human error.

- CompTIA study 2012

The Unstructured content challenge



Structured data

- Includes financial transactions, billing information, and inventory
- Typically resides in systems of records designed to handle specific types of information
- Typically managed through system access controls
- Limited need to collaborate with internal and external parties
- Lots of industry maturity around securing such data



Unstructured content

- Includes every type of corporate information including employee records, invoices, contracts, strategy documents, forecasts, intellectual property, etc.
- Tends to be “all over the place” among systems, laptops, email attachments, thumb drives
- Highly collaborative in nature (working drafts, reviews, signatures, etc.)
- Usually no “system of record”
- Low industry maturity and best practices



No one comes to work excited about spending all day complying with IT security policies

99.9% of employees just want to do a good job, and feel that onerous IT policies get in their way of being effective

IT security must be designed to be seamless to the end user, or it simply won't work (e.g. iPhone TouchID login)

Burdensome policies and onerous restrictions just encourages people to “go around the system” thereby making things less secure



things business leaders should consider to keep their digital information secure, and protect their companies



1. Change the conversation with end users

Empathize: Start with human experiences and needs

- Understand the day to day pain points and points of friction in users' daily work
- Strategize to reduce the number of end points and silos users have to navigate
- Automate decisions around where content and data should live so users don't have to

Question Assumptions and Re-think approaches

- Instead of trying to block unsanctioned usage, learn and deliver solutions that users need so they don't have to go around policies
- Instead of mandating users not use untrusted devices, find ways to keep identities and data secure on any device the user chooses to use

Seek Simplicity as a design principle for your IT environment

- Use technologies that put user centricity and design first, to make users' work simpler
- Automate ancillary tasks such as versioning, retention, notifications, search and compliance through smart defaults and policy enforcement
- Give end users as much autonomy as possible, while maintaining visibility at the enterprise level, setting "guard rails" for accepted behaviors



2. Kill the password through better access management

Centralize identities for you enterprise users

- Think about internal AND external users who need to work together to run your business
- Establish identity and access management policies – How do internal people authenticate to your systems? What about external users?
- Implement a centralized identity management system where policies are implemented and user identities “live” – Modern cloud technologies offer many cost effective options.

Implement multi-factor authentication (MFA)

- Integrate your IDM with all critical business systems and content stores
- Require one, simple, trusted MFA process for access to all corporate data
- Think about all access scenarios including access from your corporate network and outside it

Periodically audit and clean up your identities

- Automate rules around auto-account lockout after period of inactivity
- Tie user identities with your HR system of record to automatically provision and de-provision accounts
- Perform periodic audits of account activity, user behavior, and clean up as you go
- Use automated policies in your systems and tools to flag anomalous behavior



3. Let the cloud do the heavy lifting for you

Identify trusted enterprise cloud solutions for your IT environment

- Leverage Gartner, Forrester and others to understand company landscape for each area of enterprise IT you need to solve for (HR, CRM, IDM, ERP, ECM, etc.)
- Ask tough question, do pilots, talk to other customers
- Buy platforms, not tools or solutions. Your IT environment should comprise of a set of trusted platforms that work together.
- Require and review how your cloud providers meet your security expectations

Leverage economies of scale for compliance

- Leverage the investments cloud service providers have made to achieve HIPAA, FINRA, PCI, FedRAMP, etc. to bring your environment into compliance
- Leverage the scalability and cost effectiveness to reduce internal complexities and cost
- Scale up or down as your business demands without having to invest capital, while ensuring your data is private, secure and safeguarded.

Continuously monitor your cloud environment

- Require complete transparency from your providers into all user activities, logs and event notifications.



4. Make the end points as dumb as possible

Move all data out of your end points by using browser-based cloud solutions

- Reduce the risk associated with end points getting breached, lost or stolen, by ensuring no data sits on them (laptops or mobile)
- Keep all data in the cloud, accessible and used within the browser, protected through MFA
- Invest in cloud based end point management tools to enforce policies on which applications are allowed, and what data can be stored and how

Get rid of thick clients, move to the browser

- Managing thick clients open up numerous security challenges (patching, upgrades, etc.). Actively work to eliminate thick clients and end point software from your environment
- Require that your enterprise software vendors can support 100% of offered functionality in the browser and on mobile devices without additional plugins and specialized toolkits
- Train your employees to keep their data in the browser, access from anywhere, but resist the urge to download data to their local machines

Use technologies that work together in the browser

- Expect the technologies you select to work with others to provide end-end business workflows in the browser (e.g. create a document in O365, collaborate in Box, and sign with DocuSign in the browser)



5. Re-centralize to get a handle on unstructured content

Develop a content strategy for your organization

- Figure out where your corporate content should sit, who owns it, how long you should keep it, who gets to access it, and how such decisions are made
- Ensure users at all level are aware of, and understand the corporate content policy
- Use user centered design approaches to make sure the policy strikes the right balance between security and productivity

Move your corporate content into one trusted place

- Actively eliminate silos where content resides (Network File stores, email attachments, FTP servers, DVDs, Tape backups, laptop hard drives, etc.)
- Select and deploy a content platform that meets stringent content lifecycle security and compliance requirements, but allows users to collaborate, access and work on their content from anywhere
- Migrate content from the various silos into the new content platform, and assign security rights, metadata and retention policies.

Automate content policy enforcement

- Implement automated content policies that establish “guard rails” for users, without unnecessarily getting in their way of doing day to day work.



Additional resources

1. [Applying Design thinking to Enterprise Security – White Paper](#)
2. [Info-graphic – Design thinking and enterprise security](#)
3. [Secure File Sharing Basics – What every file sharing provide should have](#)
4. [De-criminalize your colleagues – How to address shadow IT in the enterprise](#)
5. [Secure Collaboration Primer – The Perils of Email attachments](#)
6. [Redefining Content Security – White Paper](#)
7. [Enterprise Trends – Cyber security in the cloud – Info-graphic](#)



Thank you

Questions

sonny@box.com