



IT Risks and Mitigations

David Raymond

Virginia Tech IT Security Office and Lab

Agenda

- Introduction
- What are the risks?
 - What have we seen?
 - Why are we a target?
 - Common IT Risks
- What can we do?
 - IT Risk Assessment process
 - Mitigation strategies
 - Other resources
- Conclusion



What have we seen here at VT?

From: VT Webmail Team <johnr6@vt.edu>

Date: Mon, Apr 4, 2016 at 8:03 AM

Subject: WARNING: VERIFY YOUR EMAIL ACCOUNT NOW!!!

To:

Dear VT Email Account User,

This message is from VT.EDU Upgrade Team. We hereby announce to you that we are running upgrade and maintenance on our server database. Your email account would be deleted from our server if it is not verified within the next 24 hours and you will be unable to access your webmail account. To avoid the deletion of your account, you are advised to verify your email account by clicking on the link below and follow the instructions.

Click the link below to verify your email Account.

<http://vt-eduwbmailvrfy.3eeweb.com/secure-verify.vt.edu.php>

Thank you.

VT Webmail Team.

© 2016 Virginia Polytechnic Institute and State University



Email: *

Username: *

Password: *

Confirm Password: *


Full Name: *

Submit



One account. All of Google.

Sign in to continue to Gmail



[Sign in](#)

☐ Stay signed in [Need help?](#)

Please enter your full email address
example@vt.edu

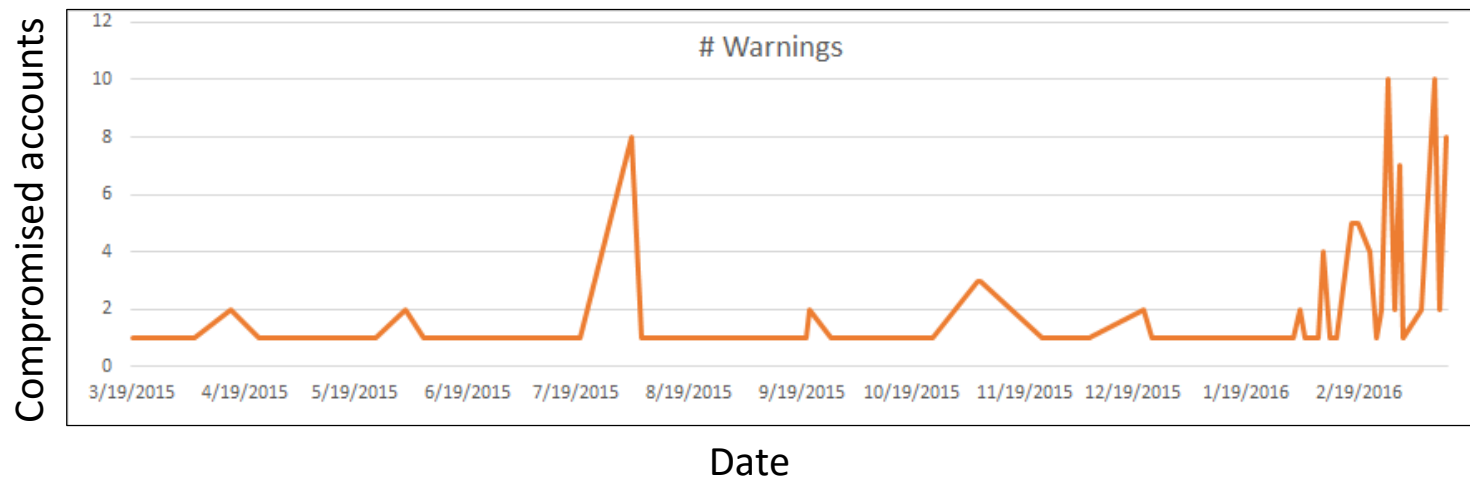
[Create an account](#)

One Google Account for everything Google



Gmail Account Compromises

- We took action in Jan/Feb to reduce system compromises leading to email spam attacks
- Attackers have changed tactics as we have made their job difficult
- Latest trend is compromised Gmail accounts
 - Fortunately this doesn't help them with spam, but *it can harm individuals whose accounts are compromised!*



Microsoft®
Outlook® Web App

Security ([show explanation](#))

- ☒ This is a public or shared computer
☐ This is a private computer
- ☐ Use Outlook Web App Light

Domain/user name:

Password:

Email:

[Log On](#)

Connected to Microsoft Exchange
Secured by Microsoft Forefront Threat Management Gateway
© 2009 Microsoft Corporation. All rights reserved.



Login to Scholar Course Management System

If you want to log in with an account other than your Virginia Tech PID, please click the following link to log in with your [Guest Account](#).

Username

Password

[Forgot username or password?](#)

☐ Warn before logging into other sites.

Login

Clear

Switch to high security [PDC login](#).

Security Notice

For security reasons, please **close** your web browser when you have finished accessing services that require authentication.



Central Authentication Service

[Help](#)

[Terms of Use](#)

[About CAS](#)

Login to Scholar Course Management System

If you want to log in with an account other than your Virginia Tech PID, please click the following link to log in with your [Guest Account](#).

Username

Password

[Forgot username or password?](#)

☐ Warn before logging into other sites.

Login

Clear

Switch to high security [PDC login](#).

Security Notice

For security reasons, please **close** your web browser when you have finished accessing services that require authentication.

Direct deposits rerouted after Illinois State University data breach

Share this article:



An attacker compromised the accounts of 13 Illinois State University (ISU) employees and diverted their direct-deposit payroll payments to another account.

The university was alerted of the **breach** Monday and later learned the attacker rerouted the payments by accessing the victims' university login information, ISU Chief of Staff Jay Groves told *The Pantagraph*.

Those affected have since had the proper amounts credited to their accounts and in order to protect the integrity of other accounts the university has temporarily suspended the ability to modify bank routing information for direct deposits online.

A total of \$50,000 was involved in the incident and the university is working with the Federal Bureau of Investigation and Illinois State Police in its investigation.

Faculty, staff and students have been instructed to check their accounts for fraudulent activity.

Groves said there have been five other universities around the country where similar incidents have occurred.



An attacker compromised the payment information of Illinois State University employees.



NPI3F1C76 / 128.173.200.142

hp LaserJet 4200

Information

Settings

Networking

CONFIGURATION

Network Settings
Other Settings
Privacy Settings
Select Language

SECURITY

Settings
Authorization
Mgmt. Protocols

DIAGNOSTICS

Network Statistics
Protocol Info
Configuration Page

Other Links

Help
Support
HP Home

Settings

Status

Wizard

Restore Defaults

Authorization

Administrator Password: ☒ Not Set ☒
Jetdirect Certificate: Installed
Access Control: Disabled

Web Interface

Encrypt All Web Communication: Disabled
Encryption Strength: Low (DES-56-bit, RC4-128-bit or 3DES-168-bit)

SNMPv1/v2

Status: Enabled
Get Community Name: Not Set (Defaults to "public")
Set Community Name: Not Set (Defaults to "public")

SNMPv3

Status: Disabled

Other Protocols

IPX/SPX: Enabled
AppleTalk: Enabled
DLC/LLC: Enabled
9100 Printing: Enabled
LPD Printing: Enabled
IPP Printing: Enabled
FTP Printing: Enabled
SLP Config: Enabled
mDNS: Enabled
Multicast IPv4: Enabled
RCFG: Enabled
Telnet: Enabled

Grade Point

Hacker sends anti-Semitic fliers to network printers at Princeton, many other colleges

A 89 Save for Later Reading List

By Mary Hui and Susan Svrluga March 29 Follow @SusanSvrluga



Princeton University. (Associated Press)

PRINCETON, N.J. — A notorious white supremacist computer hacker has claimed responsibility for sending anti-Semitic fliers to networked printers at several universities across the country, a coordinated cyberattack that

Most Read

- 1 A huge tornado killed his wife and destroyed their home. He filmed the whole thing.
- 2 9-year-old reporter breaks crime news, posts videos, fires back at critics
- 3 George Mason U. changes name of Scalia law school to avoid embarrassing acronyms
- 4 Yes, it may snow a bit in D.C. Saturday, as polar vortex unleashes parting blow
- 5 Maryland board approves \$5.6-billion Purple Line contract

Unlimited Access to The Post. Just 99¢



HP 9250C Digital Sender / 128.173.104.112
HP 9250C Digital Sender Series

Information

Settings

Digital Sending

Networking

General Settings

Send to Folder Settings

Send to Folder Address Book

Send to Folder Import/Export

E-mail Settings

E-mail Address Book

Email/Fax Import/Export

LDAP Settings

Log

Preferences

Web Service Security

General Settings

[Help](#)

This page lets you add or edit administrator settings. Click **Help** for more information.

Step 1: Enter the administrator information.

The device uses this information to send digital send job information to the administrator. ★

Name (recommended):

Mark

Phone Number (optional):

50950559809

E-mail address (recommended):

mark357177@hotmail.com ★

Location (optional):

New York

Step 2: Click Apply to save the information or click Cancel to start over without saving your changes.

Apply

Cancel

Other Links

[hp instant support](#)

[Product Support](#)

[john](#) ★

[Mark](#) ★

[gordon](#) ★



SEARCH

LET'S CHAT

START DATA RECOVERY

CASE STATUS

800.237.4200



Datarecovery.com

Services ▾

Data Loss Prevention

About

Contact

Clients

R&D

News

[View All R&D Articles](#)

Default Passwords

June 23, 2014

This page serves as a repository for the default passwords for various devices and applications.

Hardware devices listed include network devices such as routers, modems, and firewalls, along with various storage devices and computer systems. This is a substantial list, but it is not regularly updated. Revision numbers are therefore included where applicable in order to ensure accuracy.

If your device's listed password is incorrect or if you would like to submit a password for inclusion on this list, please send an email to support@datarecovery.com with this page's URL (<http://datarecovery.com/rd/default-passwords/>) in the subject line.

All of these admin passwords are provided for research purposes and for legal, legitimate use.

Manufacturer	Model/Name	Revision	Protocol	User	Password
3Com	-	1.25		root	letmein
3com	3comCellPlex7000	-		tech	tech
3COM	AccessBuilder	7000 BRI	SNMP	SNMPWrite	private
3COM	AirConnect Access	01.50-01	Multi	(none)	(none)

Categories

[COMPUTER FORENSICS](#)[DAMAGE](#)[DATA LOSS PREVENTION](#)[DATA RECOVERY KNOWLEDGE](#)[DATA RECOVERY NEWS](#)[DATA RECOVERY SERVICE](#)[DATA TYPES](#)[DATABASE](#)[EMAIL](#)[HARD DISK](#)[MAC/APPLE](#)[MEDIA](#)

UNDOCK





START CHAT

List of Default PasswordsShodan

←→↻https://www.shodan.io

ShodanDevelopersBookView All...

SHODAN




ExploreEnterprise AccessContact Us

New to Shodan?[Login or Register](#)

The search engine for the Internet of Things


Shodan is the world's first search engine for Internet-connected devices.

[Create a Free Account](#)[Getting Started](#)




Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.




See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!




Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.




Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



56% of Fortune 100



1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

NVC Server Room Temp

David

← → ↺

38.68.241.214/login

🔑

☆

...

🖨

🔍

⌵

BLACK BOX

NETWORK SERVICES

BLACK BOX ServSensor JR. v2.0

User Log Off

Location: RM 104

Current System Time: 16/3/16 16:30:39

Summary

Sensors

Traps

Mail

Network

System

Help

Auto refresh (sec.) 5 Start

Online Status of Sensors

Last Refresh: 1 mins 17 secs

Port	Type	Description	Reading	Status	Action	Graph
1	Humidity Temperature	Humidity1 Description Temperature1 Description	45 % 69 °F	Normal Normal	-	View View
2	-	-	-	-	-	-

Sys Log (240 messages)

1	16/03/16 16:29:22 User login attempt succeeded from IP address 128.173.54.125
2	16/03/16 16:13:26 User login attempt succeeded from IP address 128.173.54.118
3	16/03/16 16:13:16 Administrator login attempt failed from IP address 128.173.54.118
4	16/03/16 16:10:49 User login attempt succeeded from IP address 128.173.54.118
5	16/03/16 16:05:16 User login attempt succeeded from IP address 71.68.132.97
6	16/03/16 16:01:15 User login attempt succeeded from IP address 71.68.132.97
7	16/03/16 16:01:06 User login attempt succeeded from IP address 128.173.54.118
8	16/03/16 15:35:15 User login attempt succeeded from IP address 162.216.46.117
9	16/03/16 09:22:52 User login attempt succeeded from IP address 212.221.44.99
10	16/03/16 08:08:54 User login attempt succeeded from IP address 31.7.58.234

< Prev

Oldest

Newest

Next >

“Locky” ransomware

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

To receive your private key follow one of the links:

1. [http://\[redacted\]tor2web.org/\[redacted\]](http://[redacted]tor2web.org/[redacted])
2. [http://\[redacted\]onion.to/\[redacted\]](http://[redacted]onion.to/[redacted])
3. [http://\[redacted\]onion.cab/\[redacted\]](http://[redacted]onion.cab/[redacted])
4. [http://\[redacted\]onion.link/\[redacted\]](http://[redacted]onion.link/[redacted])

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [\[redacted\].onion/\[redacted\]](http://[redacted].onion/[redacted])
4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted] !!!



Agenda

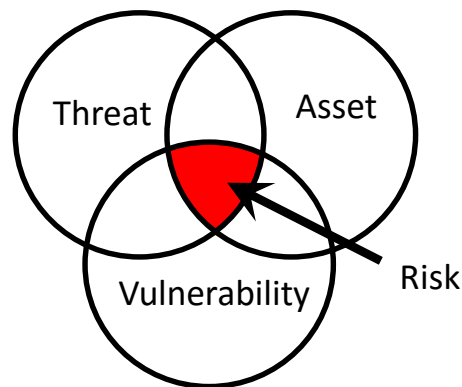
- Introduction
- What are the risks?
 - What have we seen?
 - Why are we a target?
 - Common IT Risks
- What can we do?
 - IT Risk Assessment process
 - Mitigation strategies
 - Other resources
- Conclusion

Why are we a target?

- Top tier research university
 - \$513M+ research portfolio
 - No. 1 academic research institution in VA (NSF census)
- Fairly open network architecture
 - Fosters research, collaboration, and innovation
 - Poses a common security “challenge” among colleges and universities
- High population density
 - ~40K students, staff, and faculty
 - ~100K network nodes

Other Risks

- IT Security Office provides a list of 22 potential risks to IT infrastructure
 - http://security.vt.edu/services/risk_assessment/it_risk.html
 - These are based on our observations during incident response activities and organizational security reviews
- This is a great place to start as you work to determine your risk exposure



- Asset – something of value to the organization
- Threat – possible danger to asset
- Vulnerability – weakness that leave asset open to threat

$\text{Risk} = \text{threat} \times \text{vulnerability}$

Threat: Lax or dated sysadmin practices

- Best practices should include
 - Secure system configurations
 - Periodic security audits
 - Routine backups
 - Documented and tested security settings
 - Up-to-date training
- Common failures
 - Poor/unsecure system configs
 - Lack of change control procedures
 - Failure to patch/update software
 - Inadequate data backup procedures

Risk: Inadequate desktop access control management

- Best practices
 - Review system logs for user activity and suspicious events
 - Review access rights regularly
 - Remove access rights when no longer needed
- Common failures
 - Access rights granted and never revoked
 - Logs not maintained or not reviewed

Risk: key person dependency

- Best practices
 - Cross-train personnel on critical services
 - Ensure there are backup individuals, with sufficient privileges to administer critical systems
- Common failures
 - Relying on one person to maintain critical services with not cross-training or backup personnel

Risk: Lack of strong passwords

- Best Practices
 - Use long (12 character or more) passwords
 - Use at least one each of: uppercase letters, lowercase letters, numbers, special characters
 - Do not use proper nouns, dictionary words, or usernames
 - Do not reuse passwords on multiple systems/sites
- Common failures
 - Short, easily guessed passwords
 - Password reuse
 - Passwords same as username*
 - root/root, admin/admin, ubuntu/ubuntu

*Actual username/password combinations observed on VT systems

Risk: Inadequate safeguards on sensitive data

- Best practices
 - Only store sensitive data (PII, PCI, FERPA, HIPAA, etc.) in accordance with regulatory requirements and data steward's guidance
 - Encrypt at rest and in transit
 - Understand what to do in case of data breach
 - http://security.vt.edu/resources_and_information/dealing_with_data_exposure.html
- Common failures
 - Storing more sensitive data than necessary
 - Storing sensitive data on poorly secured systems
 - Carrying unencrypted sensitive data on removable media or portable computing devices

Risk: Inadequate access control

- Best practices
 - Ensure access to resources and services are granted only to those users who are entitled to them
 - Use two-factor authentication for access control
 - Use individual accounts, not “group” accounts for system access
 - Remove access when faculty/staff/student leaves the university
- Common failures
 - Group accounts for Banner (or other) access
 - Granting access to those who don’t need it
 - Failure to audit access to sensitive data

Risk: Lack of adequate physical security

- Best practices
 - Lock office and living area doors when not present
 - Secure easily pilferable devices when not in use
 - Ensure servers and network devices are in locked cabinets
 - Minimize and monitor access to office areas
- Common failures
 - Leaving laptops, tablets, and phones unsecured when away from desk
 - Uncontrolled access to offices and labs

Risk: Natural disaster

- Best practices
 - Have completed continuity of operations plan and business impact analysis documents accessible in multiple locations
 - Use uninterruptible power supplies (UPS) and/or backup generators to mitigate loss of power to critical services
- Common failures
 - Lack of COOP, BIA

Risk: Hardware failure

- Best practices
 - Ensure critical data is backed up off site
 - Maintain records of warranty data and contacts for supported items
 - Maintain software license media and keys for re-installation
- Common failures
 - Lack of up-to-date backups
 - Failure to periodically test backup recovery process to ensure data is recoverable

Risk: Malware

- Best practices
 - Use host-based firewalls and anti-virus software to limit exposure
 - Ensure important data is backed up
 - Be prepared to wipe and reinstall system from scratch
- Common failures
 - Improperly configured or no host-based firewall
 - Lack of adequate backups

Risk: Social engineering/phishing

- Best practices
 - Employee awareness training to spread knowledge of threat
 - Block know bad senders at email portal



- Common failures
 - Lack of user awareness training



www.dilbert.com scottadams@aol.com

3-16-09 © 2009 Scott Adams, Inc./Dist. by UFS, Inc.

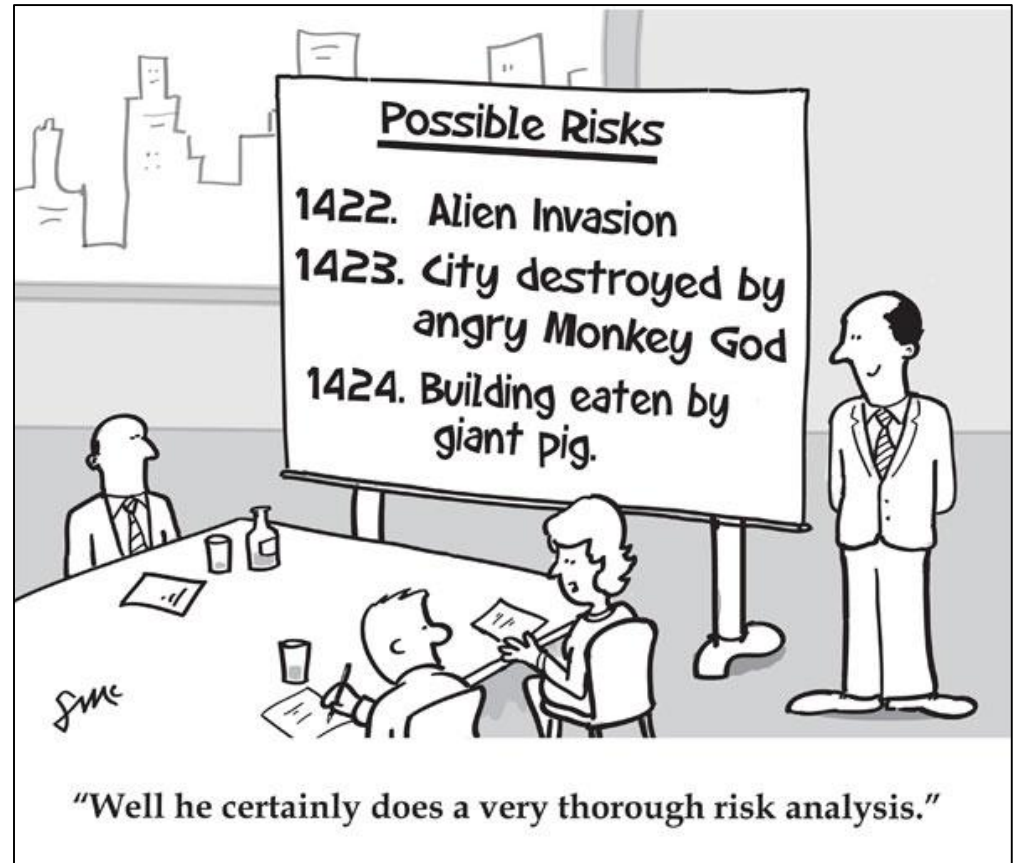


Agenda

- Introduction
- What are the risks?
 - What have we seen?
 - Why are we a target?
 - Common IT Risks
- What can we do?
 - IT Risk Assessment process
 - Mitigation strategies
 - Other resources
- Conclusion

So what do we do?

- Identify assets, prioritize, and address risks
- *You can't solve everything at once!*



Information Technology Risk Assessments

Why Conduct IT Risk Assessments?

- Helps organizations identify critical assets and risks to their IT systems
- Requires us to develop mitigations to address identified risks
- Helps ensure the continuity of critical business processes in the case of disaster or compromise
- Supports University Policy 7010 requirement for departments to “regularly analyze risks and have up-to-date recovery plans”

IT Risk Assessment is about protecting your critical business processes!

QUICKLINKS

IT Security Office

IT Security Lab

Services

IT Security Reviews

Risk Assessment

Awareness Training

Vulnerability Scanning

Web Application Scanning

Rights Management Services

All Services

Resources and Information

Students

Staff and Faculty

IT Professionals

Identity Finder

Password Change Requirements

2 Factor Authentication

About Us



IT Security Reviews

The Virginia Tech IT Security Office conducts IT security reviews throughout the university. Security reviews are a service offered by our office to help departments discover potential cyber problems that could result in improper data disclosures, illegal usage, and potential problems that weaken IT systems.

Awareness Training

The Virginia Tech IT Security Office provides training throughout the campus. Training topics cover subjects from cyber security awareness issues to the latest techniques being used to compromise IT systems.

Rights Management Services

IT Risk Assessment

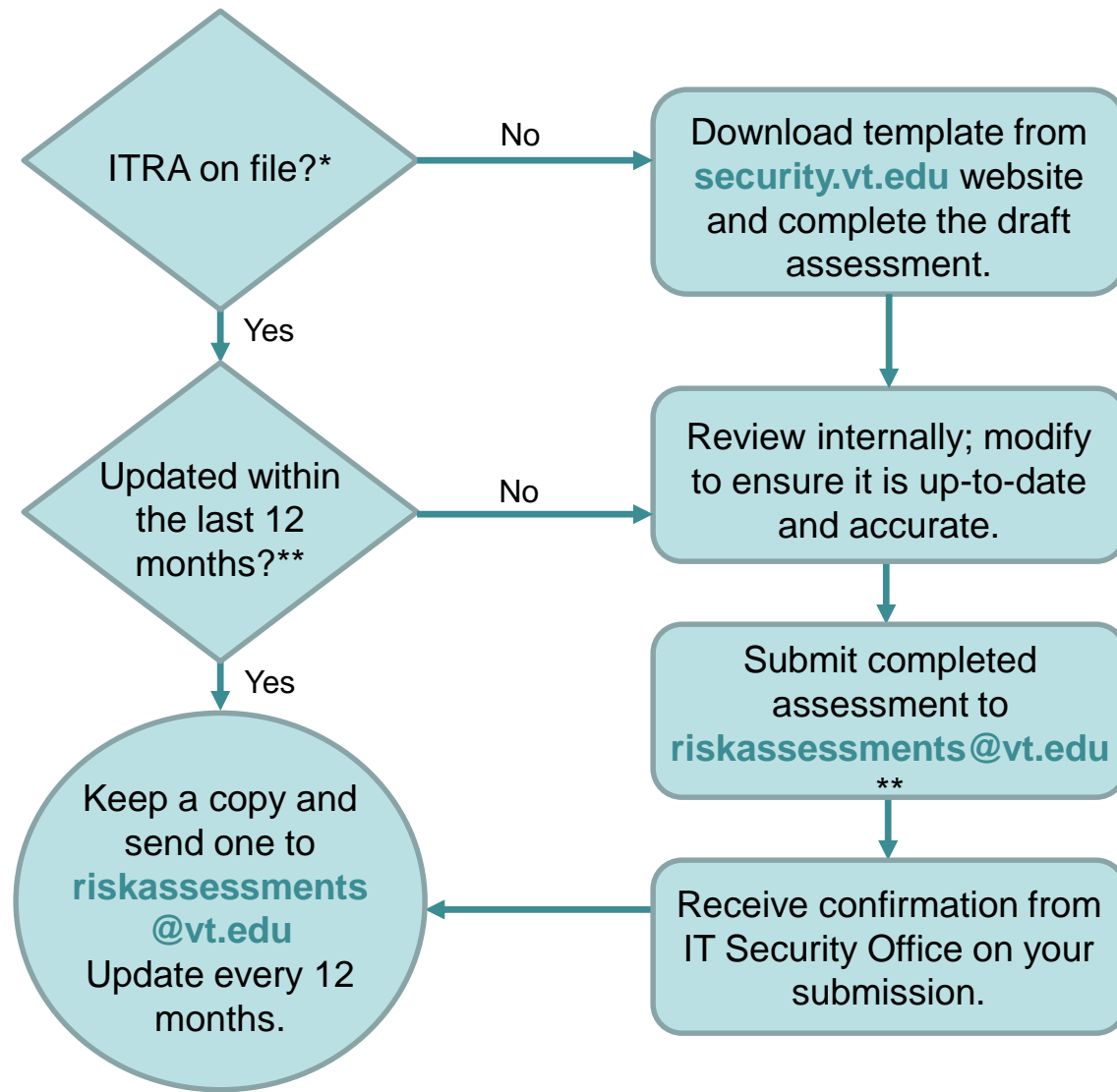
A resilient enterprise has the capacity to overcome disruptions and the ability to continually adapt to an ever-shifting range of threats and vulnerabilities. Especially in the realm of IT resources, more protection is continually required.

Web Application Scanning

The Security Office provides custom scanning for web applications. A web application scan is a specific type of vulnerability scan that is designed to address common threats to web applications.

Vulnerability Scanning

IT Risk Assessment Flow Chart, v3.0, 2015



* If the Information Technology Risk Assessment is being submitted as part of a College-level submission, please ensure that each individual department is listed and individually provides their updates to the College-level document annually.

** The IT Security Office will maintain an archive of submitted ITRA reports; departments should also retain a copy of their assessments.

Five ITRA Steps

- ❑ Step 1: Identify technology assets
- ❑ Step 2: Review and prioritize the assets
- ❑ Step 3: Identify and define risks
- ❑ Step 4: Make recommendations to mitigate the risks to critical assets
- ❑ Step 5: Document mitigations and address critical risks
 - For each mitigation:
 - Describe
 - Provide cost/benefit analysis
 - Propose implementation date
 - Select and implement chosen mitigations

Step 1: Identify IT Assets

- *Technology assets* are defined as any of the following that are important to the mission of the department:
 - Personnel
 - Hardware and software
 - Data
 - Systems and services
 - Related technology assets
- In completing step one and step two, be sure to consider:
 - ***What might be the impact if the office were to lose access to this technology resource for more than a week?***
 - Briefly describe the specific business functions, personnel, processes, research, or extension environments that exist within the department, in terms of their use of technology resources.

Step 2: Review and Prioritize

- Mission Critical
 - Highly sensitive with respect to confidentiality, integrity, or availability
 - Or*
 - If compromised, could pose a risk to life, health, and/or safety
 - Or*
 - Subject to legislative, regulatory, or contractual compliance requirements
- Essential
 - Could work around the loss of this information asset for several days
 - Eventually the asset would have to be restored to a useable status
- Normal
 - The department can operate without this information asset for an extended (though perhaps finite) period of time
 - Particular units or individuals would need to identify alternatives

Critical Asset Examples

Critical Asset Description	Examples
The asset performs a function that safeguards the life or health of members of the university community or general public.	Computing & telecommunications resources for Police/EMS dispatchers
The asset is required to support instruction in such a way that instruction could not continue without it.	Canvas, Scholar, servers for distance learning courses (IDDL)
The asset is required to provide central University business and support functions.	Registrar, bursar, controller, banner, Hokie Mart
The asset concerns data which is highly sensitive or in other ways access restricted.	Databases of personnel records; medical records.

Critical Asset Examples

Critical Asset Description	Examples
The asset performs a function that safeguards the life or health of members of the university community or general public.	Computing & telecommunications resources for Police/EMS dispatchers
The asset is required to support instruction in such a way that instruction could not continue without it.	Canvas, Scholar, servers for distance learning courses (IDDL)
The asset is required to provide central University business and support functions.	Registrar, bursar, controller, banner, Hokie Mart
The asset concerns data which is highly sensitive or in other ways access restricted.	Databases of personnel records; medical records.

Critical Asset Examples

Critical Asset Description	Examples
The asset performs a function that safeguards the life or health of members of the university community or general public.	Computing & telecommunications resources for Police/EMS dispatchers
The asset is required to support instruction in such a way that instruction could not continue without it.	Canvas, Scholar, servers for distance learning courses (IDDL)
The asset is required to provide central University business and support functions.	Registrar, bursar, controller, banner, Hokie Mart
The asset concerns data which is highly sensitive or in other ways access restricted.	Databases of personnel records; medical records.

Critical Asset Examples

Critical Asset Description	Examples
The asset performs a function that safeguards the life or health of members of the university community or general public.	Computing & telecommunications resources for Police/EMS dispatchers
The asset is required to support instruction in such a way that instruction could not continue without it.	Canvas, Scholar, servers for distance learning courses (IDDL)
The asset is required to provide central University business and support functions.	Registrar, bursar, controller, banner, Hokie Mart
The asset concerns data which is highly sensitive or in other ways access restricted.	Databases of personnel records; medical records.

Step 3: Identify and Define Risks

- Risk Definition: problems, threats, and vulnerabilities with respect to information technology assets.
 - See http://security.vt.edu/services/risk_assessment/it_risk.html
- If you identify other threats and vulnerabilities that represent unique risks to your information assets that are not covered on this list, include them in Step 3, and list those risks along with their definitions.
- Information about how to rate likelihood and impact of risks and an explanation of risk responses can be found at:
 - http://security.vt.edu/services/risk_assessment/itra_resources.html

Step 4: Recommendations to mitigate risks

For each risk pertaining to a critical asset that carries a high impact, team members should document whether:

1. Current controls are in place and enforced to mitigate risk
2. The risk can be addressed within a specific timeframe with limited impact
3. No controls will be implemented at the current time due to factors that are expected to change in the near future
 - *e.g., new software expected, pending move to new location*
4. Mitigation of the risk is not feasible, due to external factors
 - *time, budget, etc.*

Step 5: Document mitigation strategies

- Identify each solution
 - Technical or non- technical, as well as any policies or procedures that would apply.
 - Each solution should be described completely
 - If only one solution is applicable, that fact should be noted, including some discussion of why other options were dismissed
- Develop a cost/benefit analysis for each proposed solution.
 - This should include capital and direct costs, staff costs, training and support, and any other one-time or ongoing costs
- Specify a proposed implementation timeline
 - This could depend on the severity of the risk and the timeframe for implementation
- Due to ITSO on March 1st annually
 - Submit to riskassessments@vt.edu

Tips

- Think of IT Risk Assessment as helping to protect your ***Business Processes!***
 - ITRA is not a function of (solely) your IT team
- Make a realistic assessment of potential risks based on *severity* and *likelihood*
- Use ITRA as an opportunity to step back, assess potential risks, and consider all of the alternatives before a crisis situation happens



Agenda

- Introduction
- What are the risks?
 - What have we seen?
 - Why are we a target?
 - Common IT Risks
- What can we do?
 - IT Risk Assessment process
 - Mitigation strategies
 - Other resources
- Conclusion

WE SHOULD GO TO THE NORTH BEACH.
SOMEONE SAID THE SOUTH BEACH HAS
A 20% HIGHER RISK OF SHARK ATTACKS.

YEAH, BUT STATISTICALLY, TAKING
THREE BEACH TRIPS INSTEAD OF TWO
INCREASES OUR ODDS OF GETTING
SHOT BY A SWIMMING DOG CARRYING
A HANDGUN IN ITS MOUTH BY **50%**!

OH NO! THIS IS
OUR THIRD TRIP!



REMINDER: A 50% INCREASE
IN A TINY RISK IS **STILL TINY.**