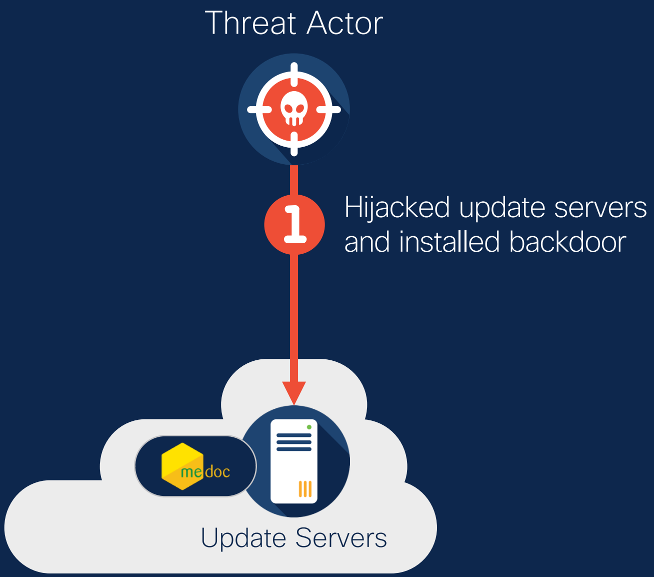
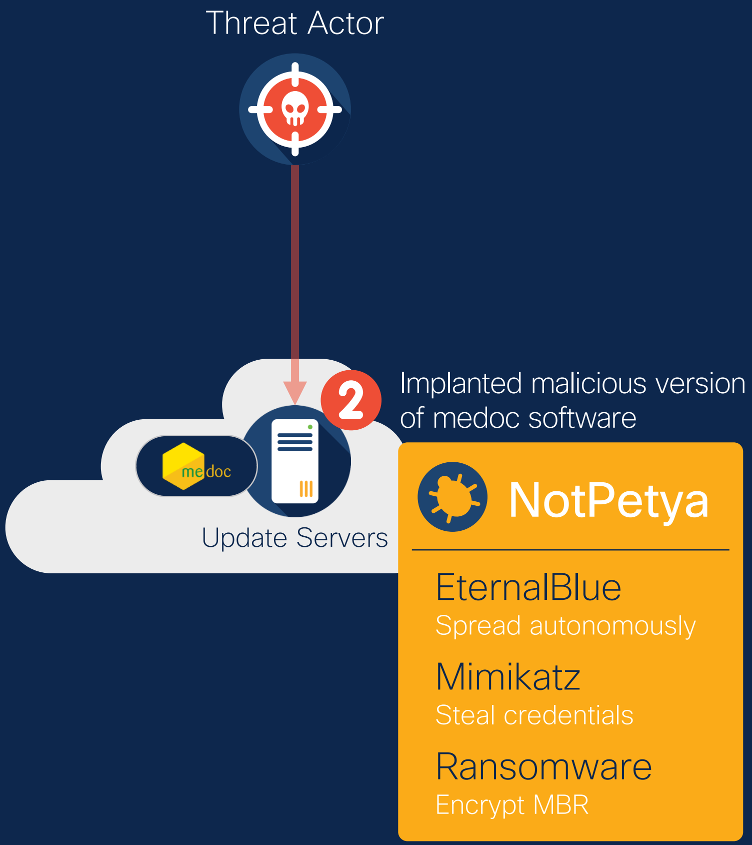
WIRED

ANDY GREENBERG SECURITY 08.22.2018 05:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.


Threat Actor
1
Hijacked update servers
and installed backdoor
me doc
Update Servers



Threat Actor

Update Servers

Implanted malicious version of medoc software

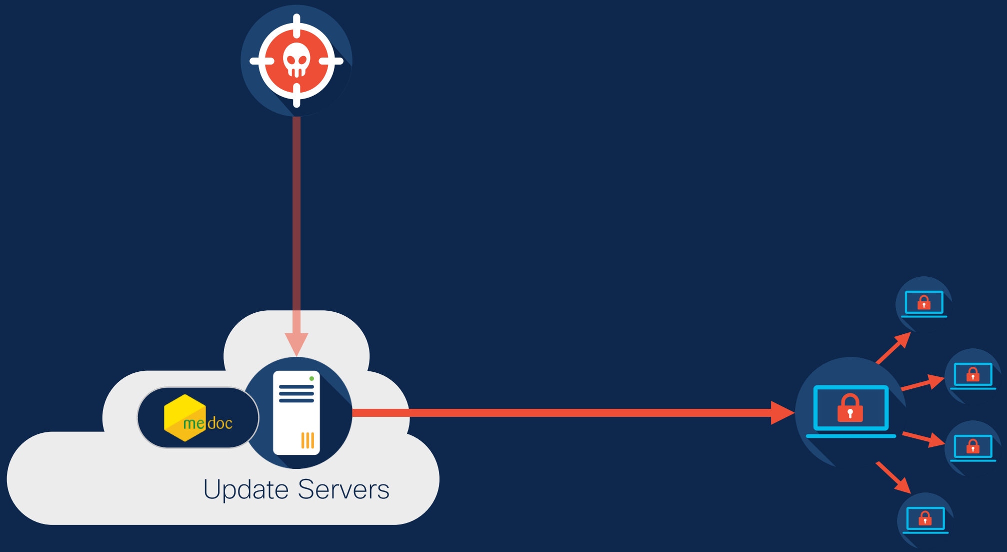
NotPetya

EternalBlue
Spread autonomously

Mimikatz
Steal credentials

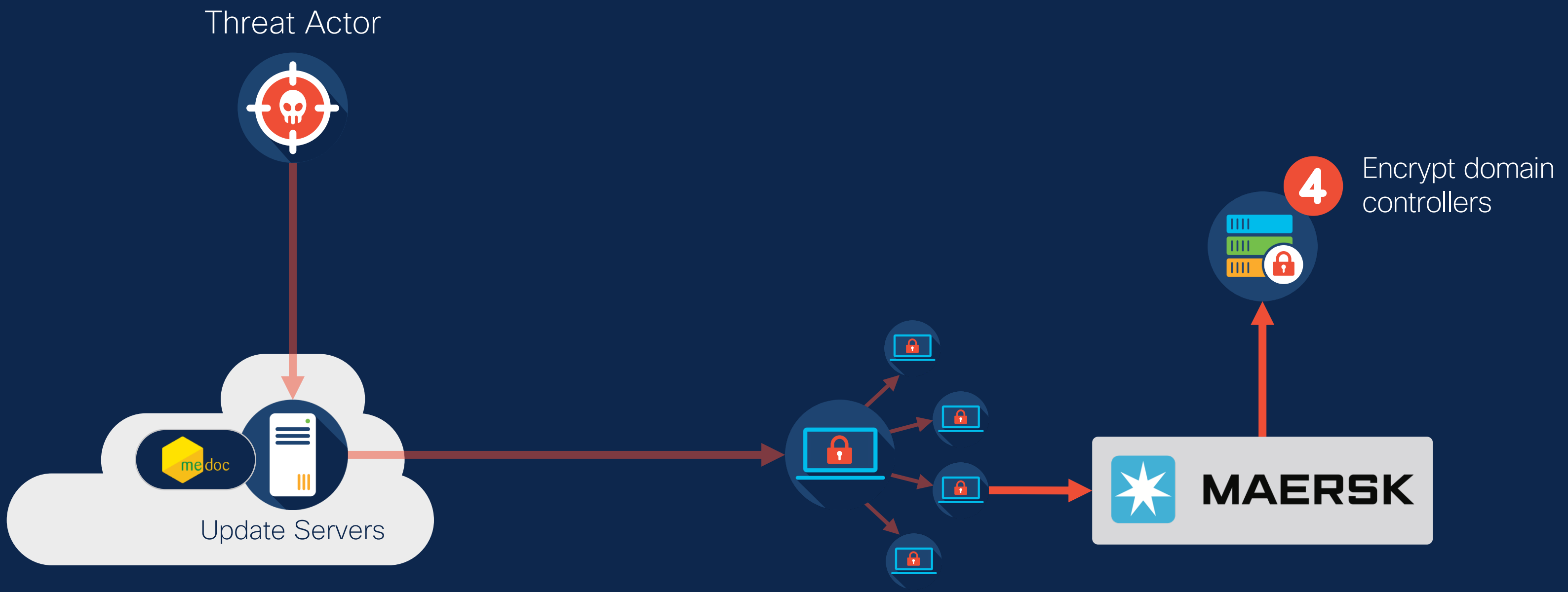
Ransomware
Encrypt MBR

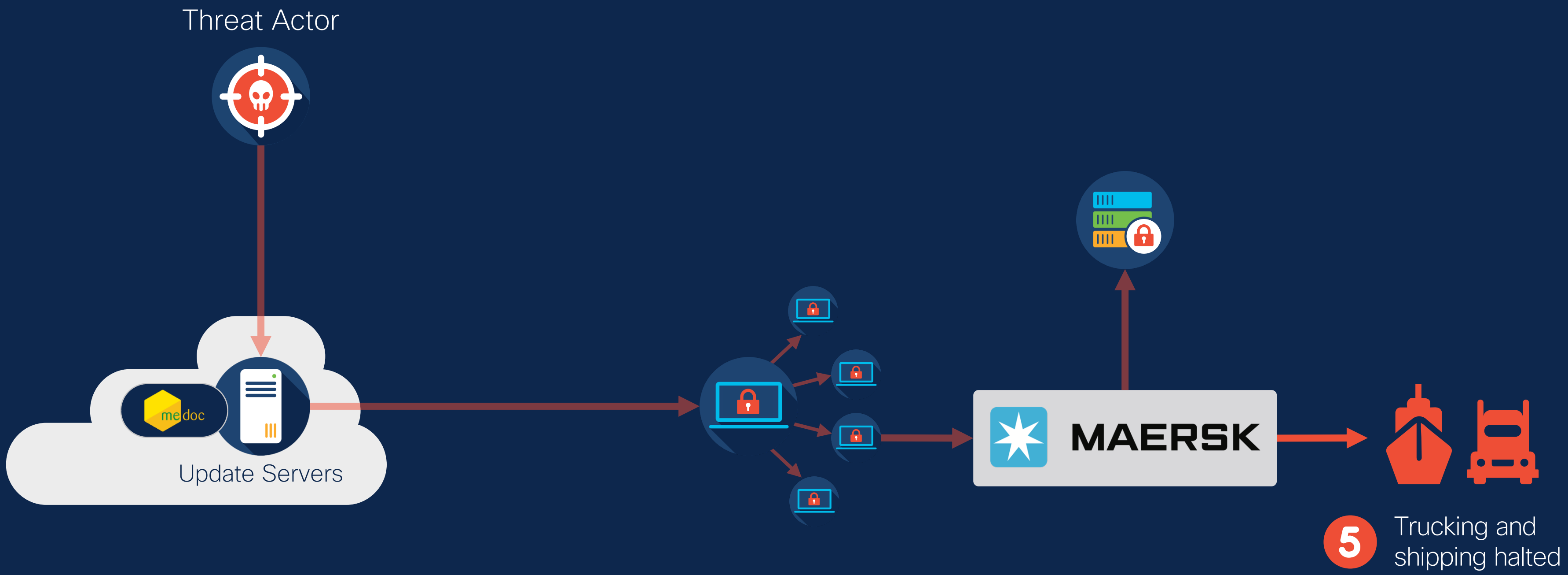
Threat Actor



Update Servers

3 Infect & spread


Threat Actor
4
Encrypt domain controllers
me doc
Update Servers
MAERSK



5 Trucking and shipping halted

$10 billion

Total damages from NotPetya, as estimated by the White House

Strengthening the Weakest Link

Becoming the Human Firewall Against Cyber Threats

Agenda

- Introduction to Cybersecurity
- Staying Safe Online

Skills for All Cybersecurity Course References

Introduction to Cybersecurity

Network Defense

Endpoint Security

Cyber Threat Management

Introduction to Cybersecurity

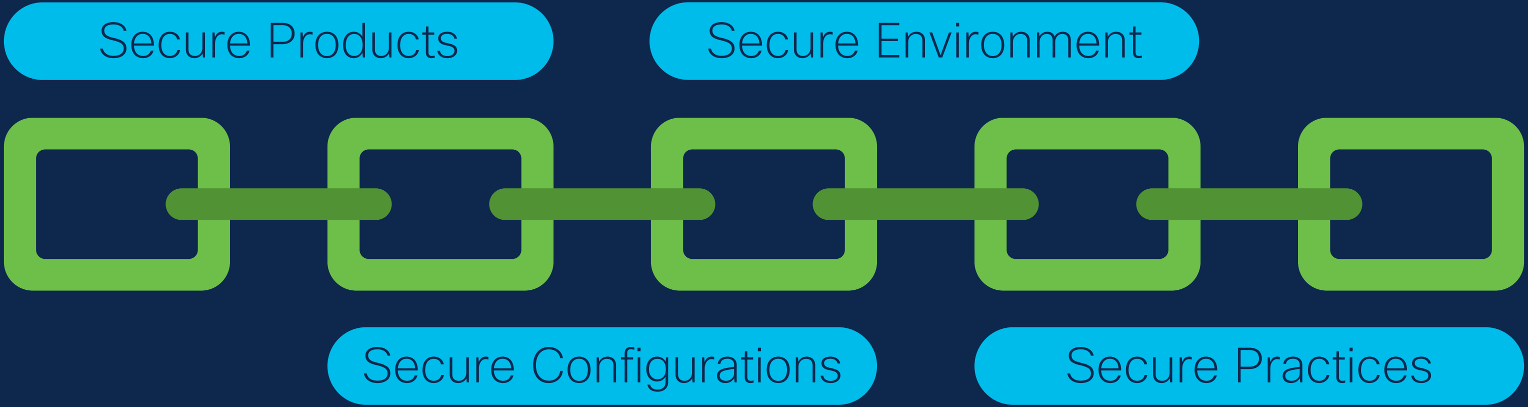
What is Cybersecurity?

> “Preservation of **confidentiality**, **integrity**, and **availability** of information.”

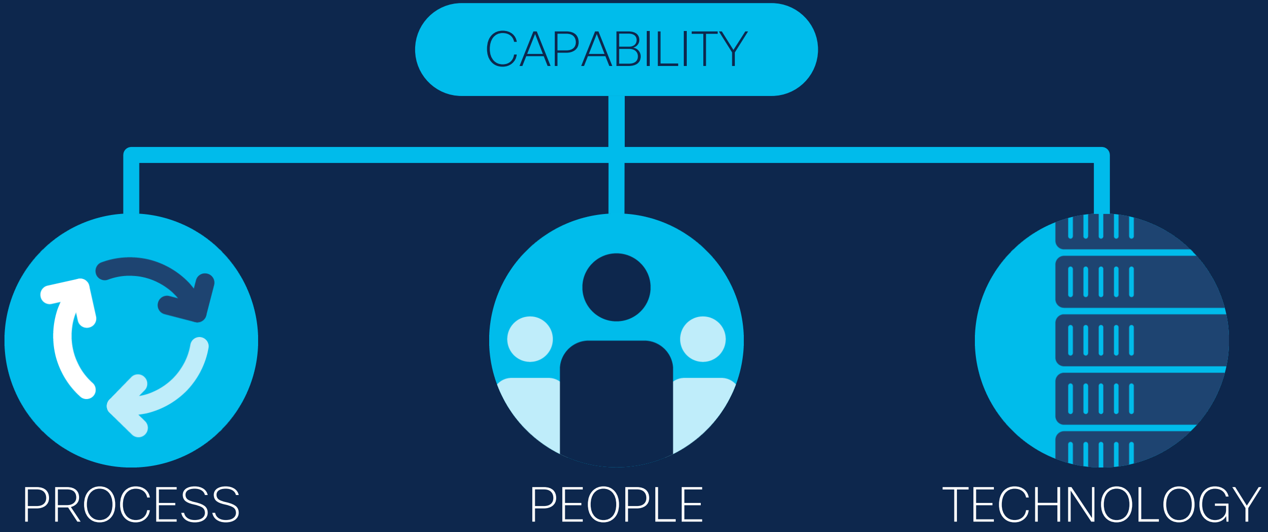
ISO/IEC 27000 – Information Security Management Systems Standard

Security as a Chain

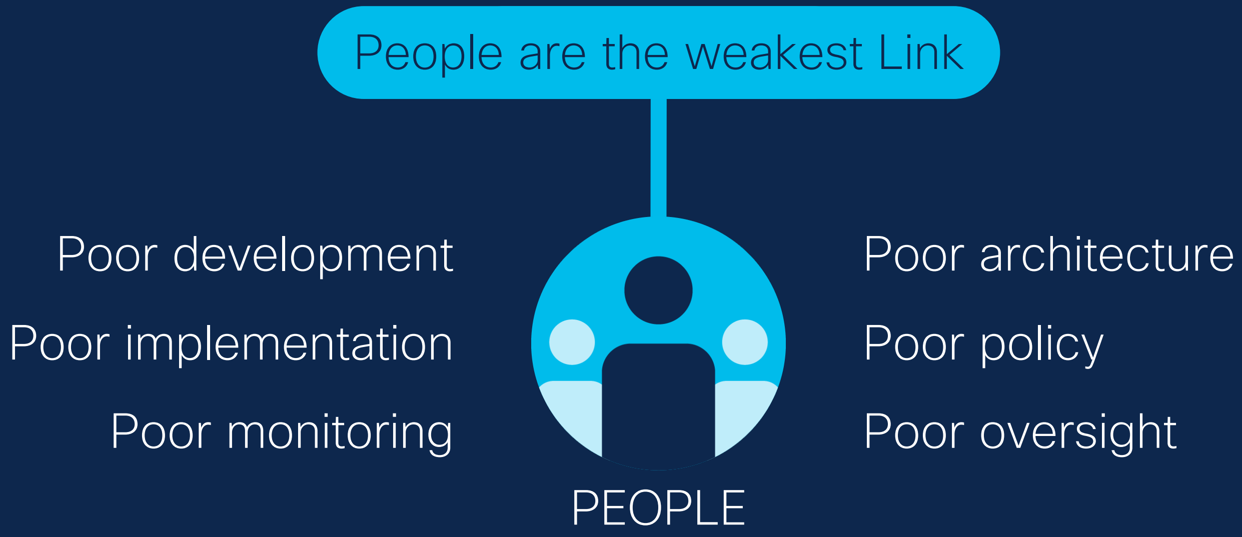
Interdependent set of **capabilities** designed to protect the confidentiality, integrity, and availability of information.



Security Capabilities



The Weakest Link



People are the weakest Link

Poor development

Poor implementation

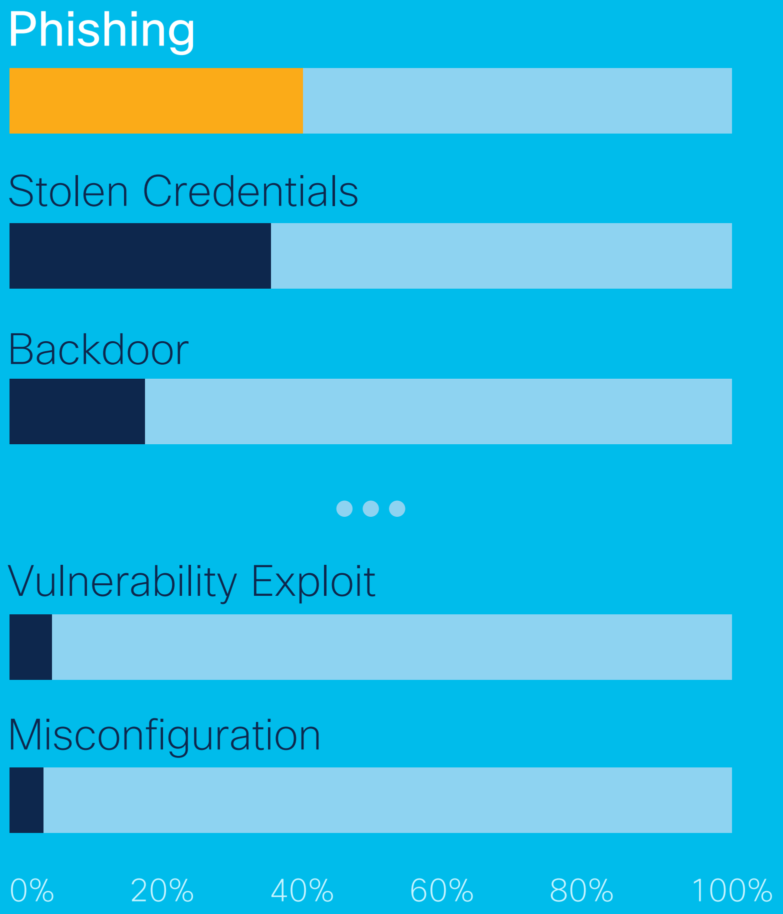
Poor monitoring

PEOPLE

Poor architecture

Poor policy

Poor oversight



32%

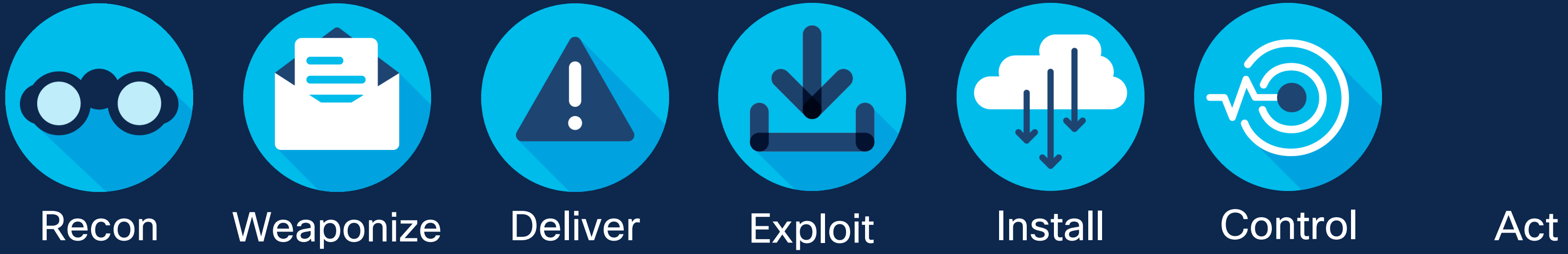
of all Breaches Involve **Phishing**

What is Cybersecurity Risk?

“The potential that a given **threat** will exploit **vulnerabilities** of an asset or group of assets and thereby cause **harm** to the organization.”

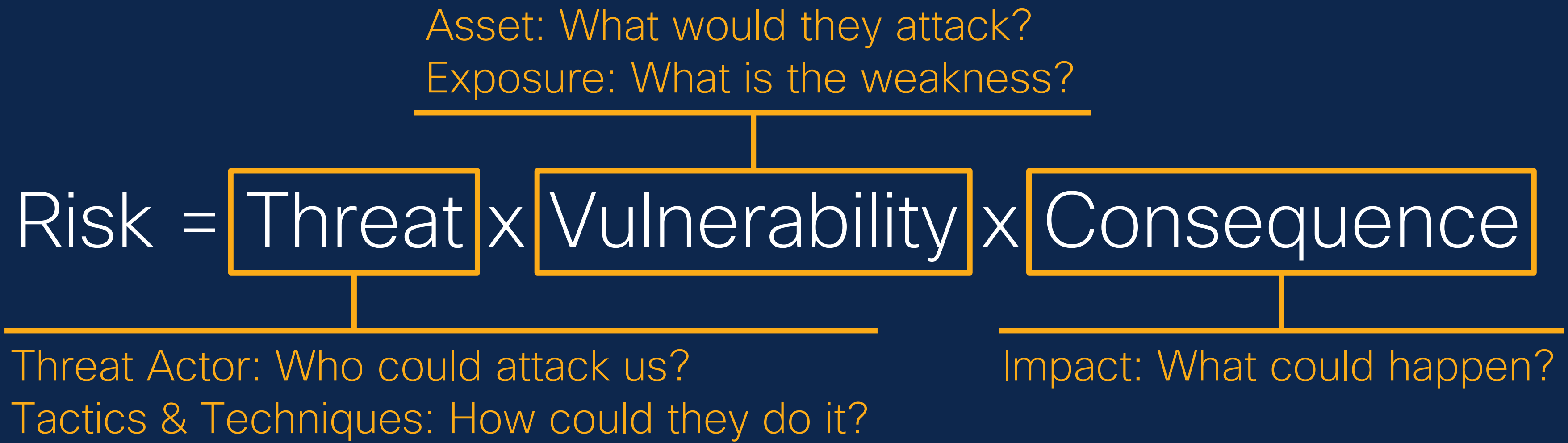
ISO/IEC 13335 – Management of Information and Communications Technology Security

The Cyber Attack Chain



Recon
Weaponize
Deliver
Exploit
Install
Control
Act

Cybersecurity Risk Formula



Asset: What would they attack?
Exposure: What is the weakness?

Risk = Threat x Vulnerability x Consequence

Threat Actor: Who could attack us?
Tactics & Techniques: How could they do it?

Impact: What could happen?

Cybersecurity Risk – Threat Actors

Nation State: Espionage, political, economic, or military

Cybercriminals: Financial gain or reputation enhancement

Hacktivists: Political, social, or ideological

Terrorist Organizations: Political, ideological, financial

Insiders: Financial gain or to seek revenge

Source: Center for Internet Security (www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors)

Cybersecurity Risk – Tactics & Techniques

Initial Access: Spearphishing, Application exploit

Execution: Run malware, Run script

Persistence: Create account, Startup items

Privilege Escalation: Bypass user account control, Memory injection

Defense Evasion: Disable security tools, Hidden files

Credential Access: Brute force, Input capture

Discovery: Network sniffing, Network scanning

Lateral Movement: Remote management, Pass the hash

Collection: Email collection, Screen capture

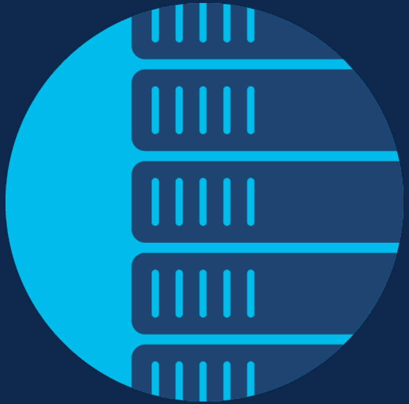
Command & Control: Data encoding, Multi-hop proxy

Exfiltration: Transfer data to cloud account, Transfer over command & control channel

Impact: Data destruction, Denial of service

Source: Mitre ATT&CK Framework (attack.mitre.org)

Cybersecurity Risk – Assets



Endpoints: User data, Account access

Network: Sniff traffic, Hijack sessions

Servers & Applications: PII, Intellectual property, etc

Cybersecurity Risk – Exposure

System Flaw: Software bug, Misconfiguration

Lack of Security: Weak password rules, Open access

Human Actions: Poor password choice, Gullibility

Organizational: Inadequate oversight, Lack of staff

Source: New York University

Cybersecurity Risk – Impact

$17.7B SGD

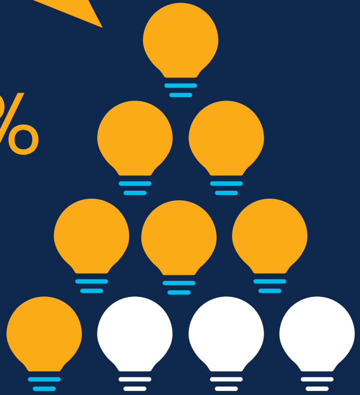
Fines · Containment · Response · Brand Impact · Loss of Jobs

Source: Frost & Sullivan study commissioned by Microsoft

Lack of Cybersecurity Hinders the Innovation Potential of Digitization

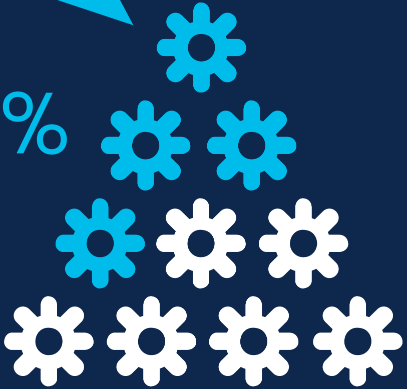
"Cybersecurity risks and threats hinder innovation in my organization."

71%



"My organization halted a mission-critical initiative due to cybersecurity concerns."

39%



Survey: 1014 respondents

> Innovations are moving forward, **but probably at 70%-80% of what they otherwise could** if there were better tools to deal with the dark cloud of cybersecurity threats.
>
> Airline Industry CFO

Staying Safe Online

How can I be a strong link?

Secure your Accounts

Click with Caution

Keep Software Up to Date

Protect your Privacy

Secure your Accounts

],^?),?3@3y$493*

e9xYb]MK.xWoB9BA

9KEjQhxD3GDy4Y*v

16 characters or more

Use long, randomized passwords for every account

Secure your Accounts

Cisco Networking Academy Verified Introduction to Cybersecurity

],^?),?3@3y$493*
e9xYb]MK.xWoB9BA
9KEjQhxD3GDy4Y*v

16 characters or more

1Password

Dashlane

LastPass

Use a password manager

Secure your Accounts

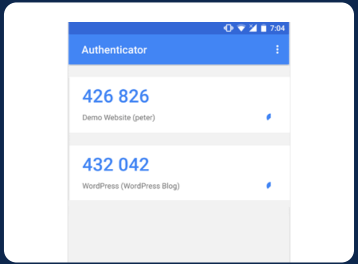
],^?),?3@3y$493*
e9xYb]MK.xWoB9BA
9KEjQhxD3GDy4Y*v

16 characters or more

1Password

Dashlane

LastPass •••|



426 826
Demo Website (peter)

432 042
WordPress (WordPress Blog)

Use multi-factor authentication wherever available

Secure your Accounts

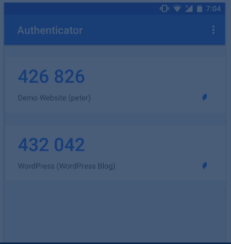
],^?),?3@3y$493*
e9xYb]MK.xWoB9BA
9KEjQhxD3GDy4Y*v

16 characters or more

1Password

Dashlane

LastPass •••|

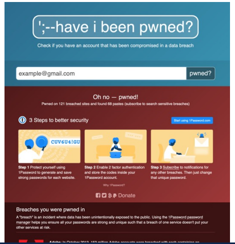


7:04

Authenticator

426 826
Demo Website (peter)

432 042
WordPress (WordPress Blog)



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

example@gmail.com | pwned?

Oh no — pwned!

Pwned on 121 breached sites and found 68 pastes (subscribe to search sensitive breaches)

3 Steps to better security | Start using 1Password.com

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?

Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Change your password if you suspect compromise

https://haveibeenpwned.com

Secure your Accounts

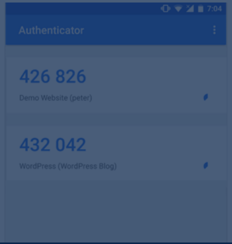
],^?),?3@3y$493*
e9xYb]MK.xWoB9BA
9KEjQhxD3GDy4Y*v

16 characters or more

1Password

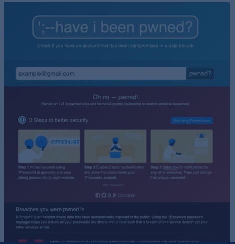
Dashlane

LastPass •••|



426 826
Demo Website (peter)

432 042
WordPress (WordPress Blog)



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Oh no — pwned!

Pwned on 121 breached sites and found 68 pastes (subscribe to search sensitive breaches)

3 Steps to better security

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Mother's maiden name?
Oiafm3ianifn

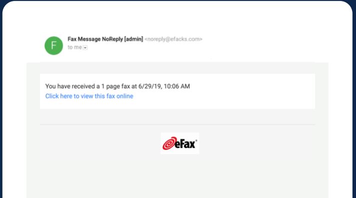
First car?
Lijwliffg 34934

Favorite Airline?
Flipfloppy Air

Use random answers for security questions

(and store them in your password manager)

Click with Caution



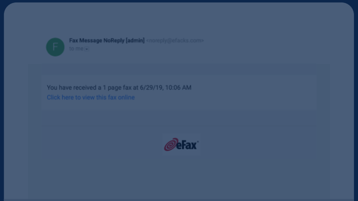
Fax Message NoReply [admin] <noreply@efacks.com>
to me

You have received a 1 page fax at 6/29/19, 10:06 AM
Click here to view this fax online

Fax Service?

Be skeptical: What is the source? Is this plausible?

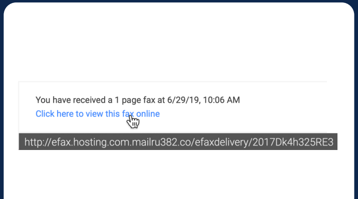
Click with Caution



Fax Message NoReply [admin] <noreply@efacks.com>
to me

You have received a 1 page fax at 6/29/19, 10:06 AM
Click here to view this fax online

Fax Service?



You have received a 1 page fax at 6/29/19, 10:06 AM
Click here to view this fax online

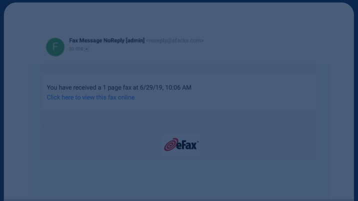
http://efax.hosting.com.mailru382.co/efaxdelivery/2017Dk4h325RE3

mailru382.co?

PC: Hover over link
iOS: Long press link and view in share sheet
Android: Copy link and paste in note app

Preview URL before opening link

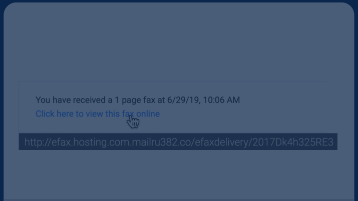
Click with Caution



Fax Message NoReply [admin] <noreply@efacks.com>
to me

You have received a 1 page fax at 6/29/19, 10:06 AM
Click here to view this fax online

Fax Service?



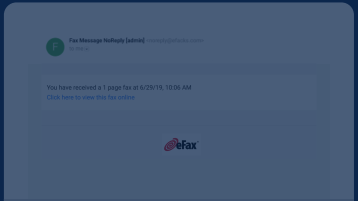
You have received a 1 page fax at 6/29/19, 10:06 AM
Click here to view this fax online

http://efax.hosting.com.mailru382.co/efaxdelivery/2017Dk4h325RE3

mailru382.co?

When in doubt, throw it out

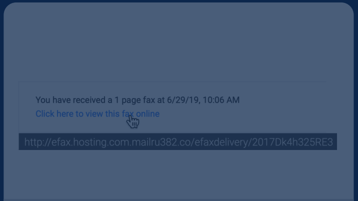
Click with Caution



Fax Message NoReply [admin] <noreply@efacks.com>
to me

You have received a 1 page fax at 6/29/19, 10:06 AM
Click here to view this fax online

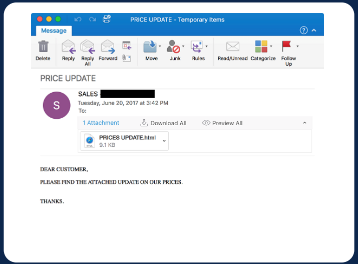
Fax Service?



You have received a 1 page fax at 6/29/19, 10:06 AM
Click here to view this fax online

http://efax.hosting.com.mailru382.co/efaxdelivery/2017Dk4h325RE3

mailru382.co?



PRICE UPDATE

SALES [redacted]
Tuesday, June 20, 2017 at 3:42 PM
To:

1 Attachment Download All Preview All

PRICES UPDATE.html
9.1 KB

DEAR CUSTOMER,

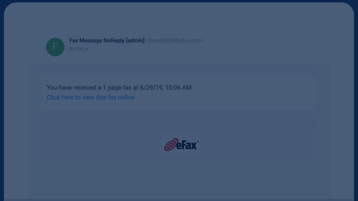
PLEASE FIND THE ATTACHED UPDATE ON OUR PRICES.

THANKS.

Avoid launching email attachments

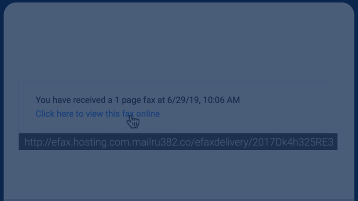
Click with Caution

Cisco Networking Academy Verified Introduction to Cybersecurity


Fax Message NoReply [admin] <noreply@efacks.com>
to me

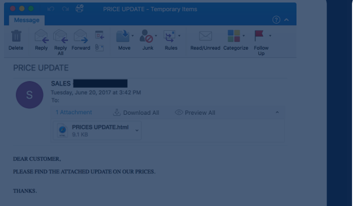
You have received a 1 page fax at 6/29/19, 10:06 AM
Click here to view this fax online

Fax Service?


You have received a 1 page fax at 6/29/19, 10:06 AM
Click here to view this fax online

http://efax.hosting.com.mailru382.co/efaxdelivery/2017Dk4h325RE3

mailru382.co?



PRICE UPDATE

SALES [redacted]
Tuesday, June 20, 2017 at 3:42 PM
To:

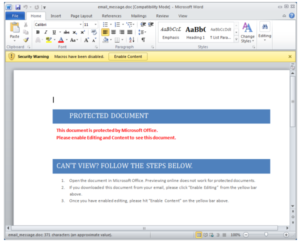
1 Attachment · Download All · Preview All

PRICES UPDATE.html
9.1 KB

DEAR CUSTOMER,

PLEASE FIND THE ATTACHED UPDATE ON OUR PRICES.

THANKS.



Security Warning Macros have been disabled. Enable Content

PROTECTED DOCUMENT

This document is protected by Microsoft Office.
Please enable Editing and Content to see this document.

CAN'T VIEW? FOLLOW THE STEPS BELOW.

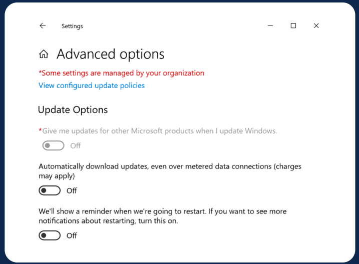
1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please hit "Enable Content" on the yellow bar above.

email_message.doc: 371 characters (an approximate value).

100%

Don't run macros in office documents

Keep Software Up to Date



Advanced options

*Some settings are managed by your organization

View configured update policies

Update Options

*Give me updates for other Microsoft products when I update Windows.

Off

Automatically download updates, even over metered data connections (charges may apply)

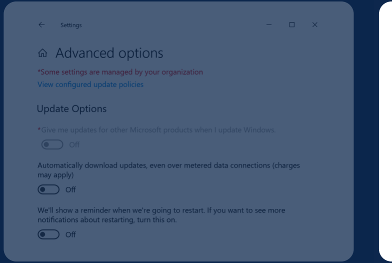
Off

We'll show a reminder when we're going to restart. If you want to see more notifications about restarting, turn this on.

Off

Enable auto update features

Keep Software Up to Date



Settings

Advanced options

*Some settings are managed by your organization

View configured update policies

Update Options

*Give me updates for other Microsoft products when I update Windows.

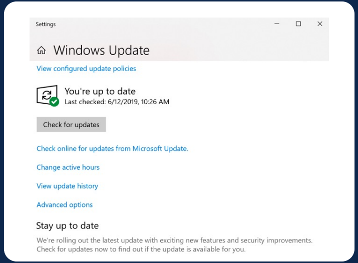
Off

Automatically download updates, even over metered data connections (charges may apply)

Off

We'll show a reminder when we're going to restart. If you want to see more notifications about restarting, turn this on.

Off



Settings

Windows Update

View configured update policies

You're up to date
Last checked: 6/12/2019, 10:26 AM

Check for updates

Check online for updates from Microsoft Update.

Change active hours

View update history

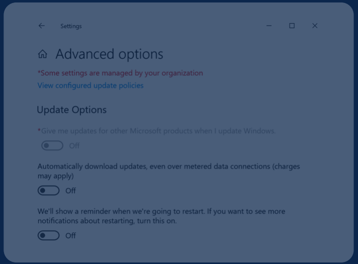
Advanced options

Stay up to date

We're rolling out the latest update with exciting new features and security improvements. Check for updates now to find out if the update is available for you.

Regularly check for application updates

Keep Software Up to Date



Advanced options

*Some settings are managed by your organization

Update Options

*Give me updates for other Microsoft products when I update Windows.

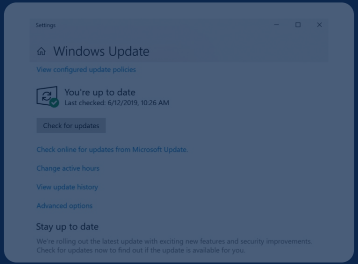
Off

Automatically download updates, even over metered data connections (charges may apply)

Off

We'll show a reminder when we're going to restart. If you want to see more notifications about restarting, turn this on.

Off

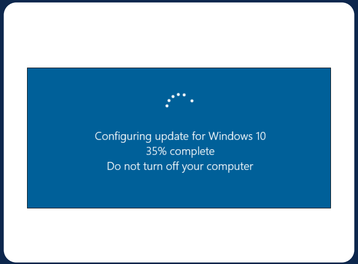


Windows Update

You're up to date
Last checked: 6/12/2019, 10:26 AM

Stay up to date

We're rolling out the latest update with exciting new features and security improvements. Check for updates now to find out if the update is available for you.


Configuring update for Windows 10
35% complete
Do not turn off your computer

Apply updates as soon as possible

Protect your Privacy

Assume everything you put online is public

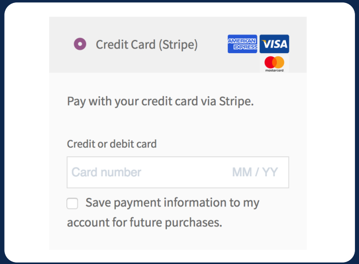
Protect your Privacy

Use VPNs on WiFi Hotspots (or always!)

Protect your Privacy

Disable WiFi and Bluetooth to avoid tracking

Protect your Privacy



● Credit Card (Stripe)

Pay with your credit card via Stripe.

Credit or debit card

Card number MM / YY

□ Save payment information to my account for future purchases.

Don’t save credit card data online

Conclusion

Takeaways

- Take the time to understand and follow your organizational security policies

- Protect yourself and your organization: Secure Accounts, Click with Caution, Update Software, Protect Privacy

- Join the fight: Cybersecurity is a great career opportunity!

CISCO