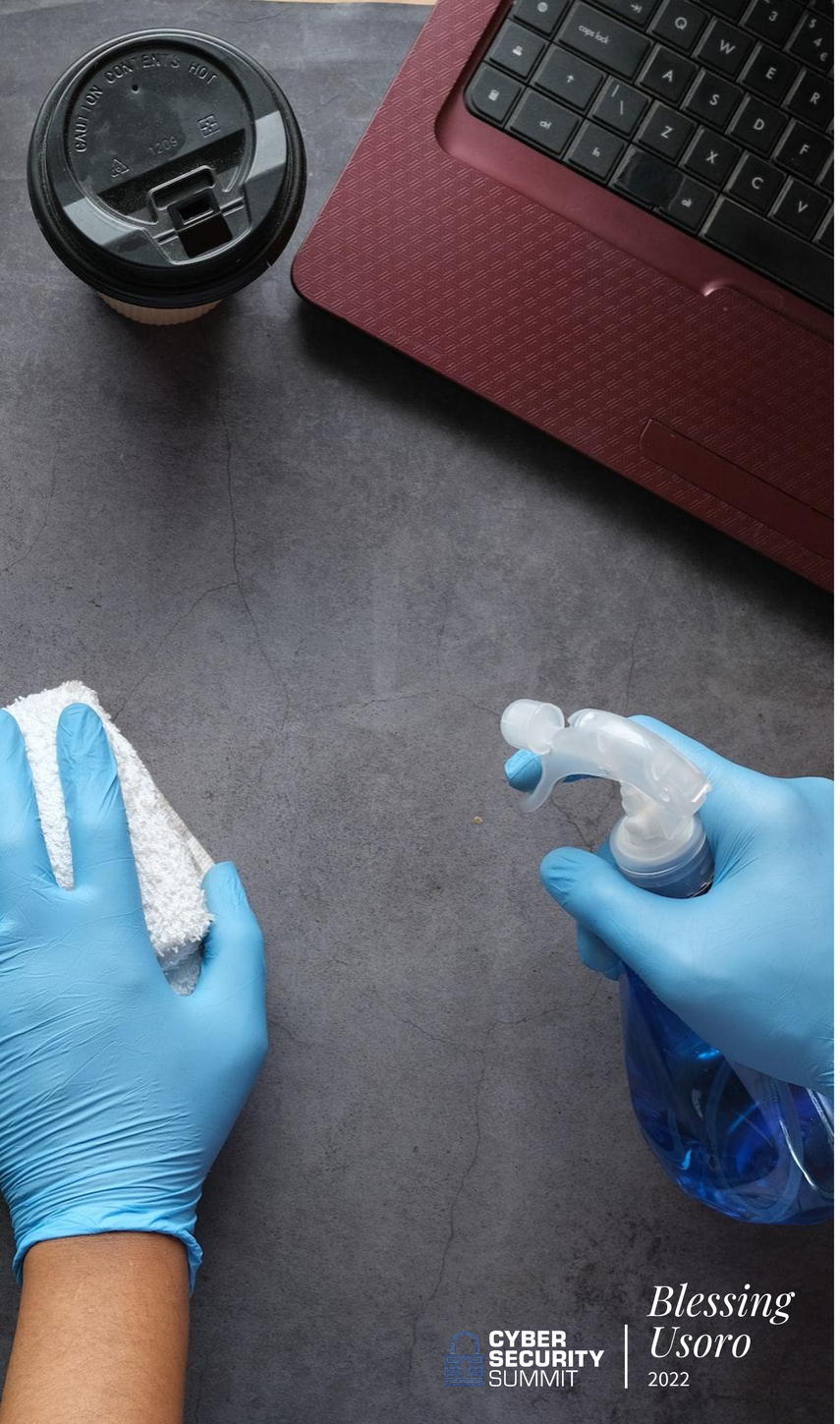
Cyber Hygiene:

Why are companies failing the basics?

CYBER SECURITY SUMMIT

Blessing Usoro

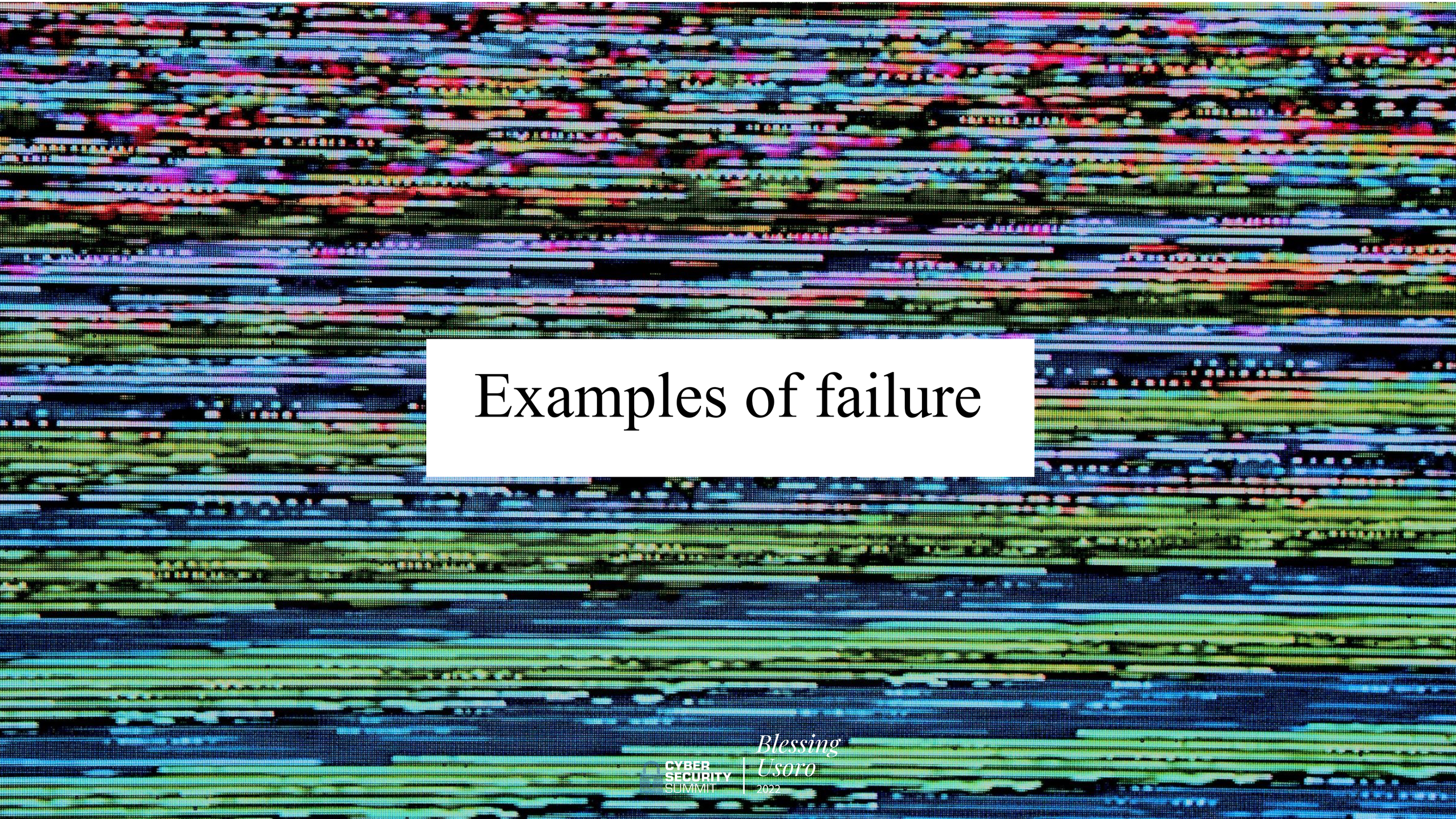
2022



What is Cyber Hygiene?

"Cyber hygiene is a set of habitual practices for ensuring the safe handling of critical data and for securing networks. It's like personal hygiene, where you develop a routine of small, distinct activities to prevent or mitigate health problems.

A fundamental principle of cyber hygiene is that it becomes part of everyday routine."


Examples of failure

Former admin borks ex-employer's network to try to get his job back with a raise

You can't make this stuff up

By Cal Jeffrey September 30, 2022 at 4:31 PM | 11 comments

Not his real face!

Casey works for a financial firm as an IT Administrator

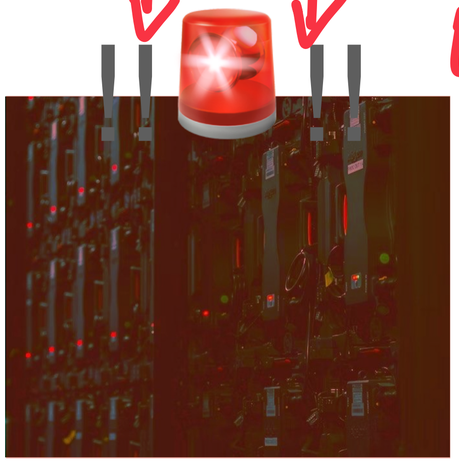
But he gets fired in 2019

He tries to log back on to his former employer's systems and realises he still has admin access

He plots revenge, not only is he going to get his job back, he'll be paid more too

He gets pissed

Casey made critical changes that shut down email and the corporate websites. Then he locked out other admins.



Eventually the FBI, stepped in and Casey got caught. He'll be sentenced January 2023

THE END

What lesson can we learn here?

Improper Offboarding Poses Significant Security Risks

The problem

48% 48% of organisations said they are aware that former employees still have access to corporate networks.

20% 20% of organisations say they've experienced a data breach that's linked to former employees

Offboarding and deactivating a user's account can be a manual and time-consuming process.

It is also very time-sensitive and sometimes requires IT admins to be available at a moment's notice.

How to fix it

📝 **Create an Offboarding Checklist**
Deactivation of ALL applications: Email, Slack, teams, File shares, VPN, etc

🗣️ **Establish a continuous communication with HR**
Does HR inform the IT team in a timely manner when an employee leaves?
Is there an email group for communication between the IT team and HR?

🔎 **Find the right Right Identity Provider**
Allows you to automate deactivation of a user's identity.
Lets you easily and quickly revoke access to ALL resources.

[redacted] Discloses Insider Attack, 8,000 Affected by Breach

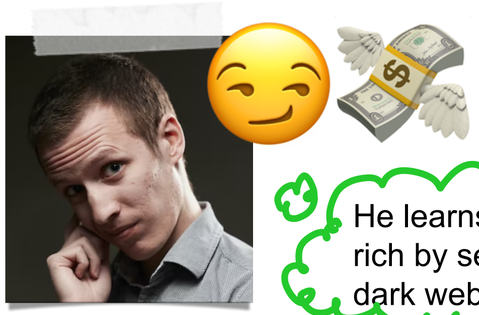
by [redacted]

posted on
June 8, 2018

0

Aiden works for a certain beverage company.

BEVERAGE COMPANY



He learns that you can get rich by selling data on the dark web.

So he plugs in his USB-C SSD, accesses a confidential folder and copies data belonging to 8000 of his fellow employees to be sold.

He thought he got away with it.

Until law enforcement caught him with the SSD in his possession.

What lesson can we learn here?

Not practicing least privilege access

The problem

Aiden should never have been able to access the confidential data folder.

Review user access privileges
Create structures and failsafes that allow users the least possible privilege to carry out their role.

Allowing unknown storage devices access the network

The problem

Aiden should never have been able to copy the data in the folder and his USB SSD shouldn’t have worked.

Review physical port privileges
Leverage technology to implement system-wide polices that prevent unknown USB and other devices from accessing an endpoint. Deny by default. Prevent the copying of data from specified software and locations.


Uber

How can companies get started?

Creating a Cyber Hygiene Policy

WHAT GOES IN IT

- Employ device encryption
- Update Password regularly according to convention
- Ensure Secure Authentication and Access
- Back up regularly and test back up regularly
- Regular Logging and Monitoring
- Maintaining an inventory of all network assets

Security is everyone's business.

Companies

Maintain cyber hygiene checklists, policies and routine training for employees.

Be proactive. Don't wait for something to happen.

Invest in org structures and technology that make it easier to maintain and enforce cyber hygiene.

Employees

Avoid using company's device/email account for personal use (shopping/downloading games).

Practice good cyber hygiene when WFH (only connect to trusted Wi-Fi).

Be sure to familiarise yourself with your company's cyber policies and abide by them.

cyber for schoolgirls

Cyber for Schoolgirls is a charity organization dedicated to reducing the gender gap in the cybersecurity industry in Ireland. We do this by creating awareness & encouraging schoolgirls to take up an interest in a cybersecurity career path.

Follow us on LinkedIn

linkedin.com/company/cyberforschoolgirls

Email for collaborations

blessing@cyberforschoolgirls.com

Connect with me

linkedin.com/in/blessingausoro

work@blessingusoro.com