Opening Keynote: Cybersecurity, Incident Response Tabletop

School Administrators of Montana

Ross Lemke
Director
Privacy Technical Assistance Center (PTAC)

United States Department of Education
Privacy Technical Assistance Center

What is

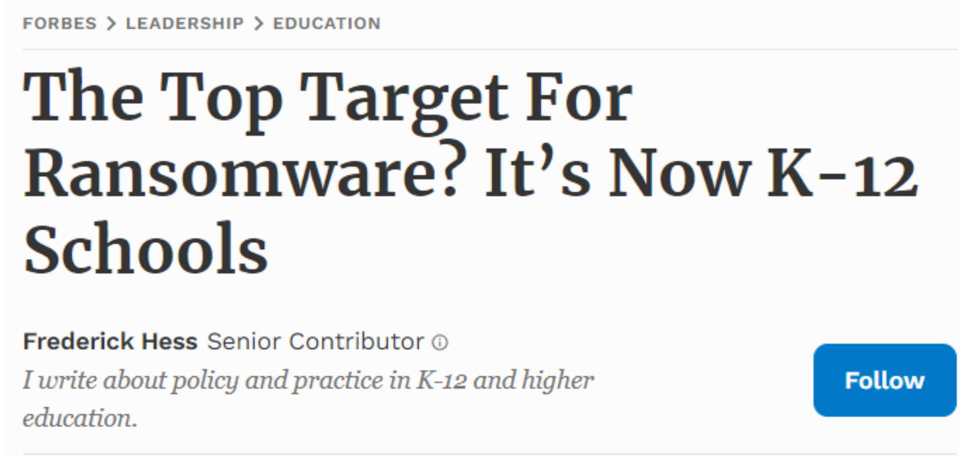
A. Your sc d new 0-
day vul ata breach

B. Your or yber
crimina of a year
hack int

C. Someo eir
passwo

Education: THE Most Targeted Sector

- 30% increase in cyberattacks on schools
- ~650k students impacted in 2021 alone
- Targeted more than healthcare and government



FORBES > LEADERSHIP > EDUCATION

The Top Target For Ransomware? It's Now K-12 Schools

Frederick Hess Senior Contributor ⓘ

I write about policy and practice in K-12 and higher education.

Schools Are the Most Targeted Industry by Ransomware Gangs

Posted on September 20, 2023 by Dissent

Waqas reports that based on research by Sophos, the education sector is the most vulnerable and targeted by ransomware attacks.

KEY FINDINGS

- 80% of lower education providers and 79% of higher education institutions reported ransomware attacks in the last year.
- Education is the most targeted industry by cybercriminals, primarily motivated by the high percentage of schools choosing to pay the ransom.
- The recovery costs from ransomware attacks have remained steady at around $1.59 million in 2023 and 2022 for lower education providers, while recovery costs in higher education have decreased significantly from the $1.42 million reported last year to just over $1 million in 2023.
- Education providers lack the funds that large corporations have to invest in robust cybersecurity measures and even staff training, leading to many loopholes sophisticated hacker groups can exploit.
- The Biden-Harris Administration has announced a $200 million initiative over three years to bolster cyber defences in K-12 schools.

Read more at HackRead.

Cliff's Notes: You're Gonna Get Hit

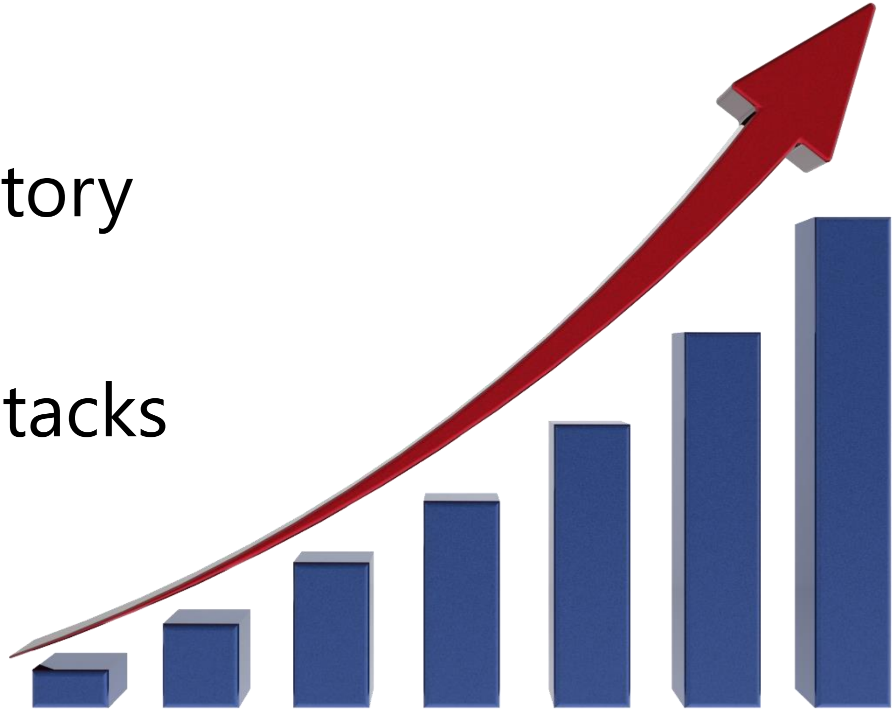
- Education == Retail and Finance
- **Employees** and **Staff** are going to be the way in
- If it isn't Ransomware, its going to be DDoS
- Spend **Time** and **Resources** on **training**
- Response plans and processes better be tailored to meet these threats

Schools are not JUST Schools

- More than just student data
- Health, family, financial data
- Employee data
- Sensitive Research data
- Other agencies' data
- Payment / Commerce data

Data Breach Impacts to Education

- Billions of dollars in costs
- Downtime from days to weeks
- Legal liabilities & regulatory penalties
- Further targeting and attacks
- Reputational harm



Many Laws May Apply

- FERPA
- IDEA
- Higher Education Act (HEA)
- GLBA implications & other applicable financial laws
- State Laws

FERPA & Data Security

What specific technology controls does FERPA require for your IT systems?

FERPA & Data Security

Yup… Nada… Nothing… Zilch…

FERPA & Data Security

Why doesn’t FERPA tell me **how** to protect student records?

Things that Happened in 1974

FERPA

Family Educational
Rights & Privacy Act

FERPA & Data Security

While FERPA doesn’t specify what security controls & technology, it does require you to protect PII from student records from disclosure and to:

- *Ensure that school officials obtain access to only those education records in which they have legitimate educational interests*
- *Identify and authenticate the identity of parents, students, school officials, and any other parties to whom the agency or institution discloses PII from education records*
- *Ensure to the greatest extent practicable that any entity or individual designated as its authorized representative uses, protects, and maintains / destroys data in accordance with FERPA requirements*

FERPA & Data Security

- “Secure” doesn’t exist
- Data security is all about managing risk
- No one is 100% patched
- Nobody can predict the 0-day attack

Understanding the Threat

Key points to understand:

1. Data **<u>will</u>** get breached
2. You will **<u>never</u>** have enough resources to be “secure”
3. It is about **<u>how</u>** you prepare

The Internet is Bad Neighborhood

Your data is only milliseconds away from every jerk on the planet

- *Malware / Ransomware*
- *Phishing & Social Engineering*
- *Hackers*
- *Denial of Service*
- *Those guys who comment bomb your social media status*

Understanding the Threat – K12

≠

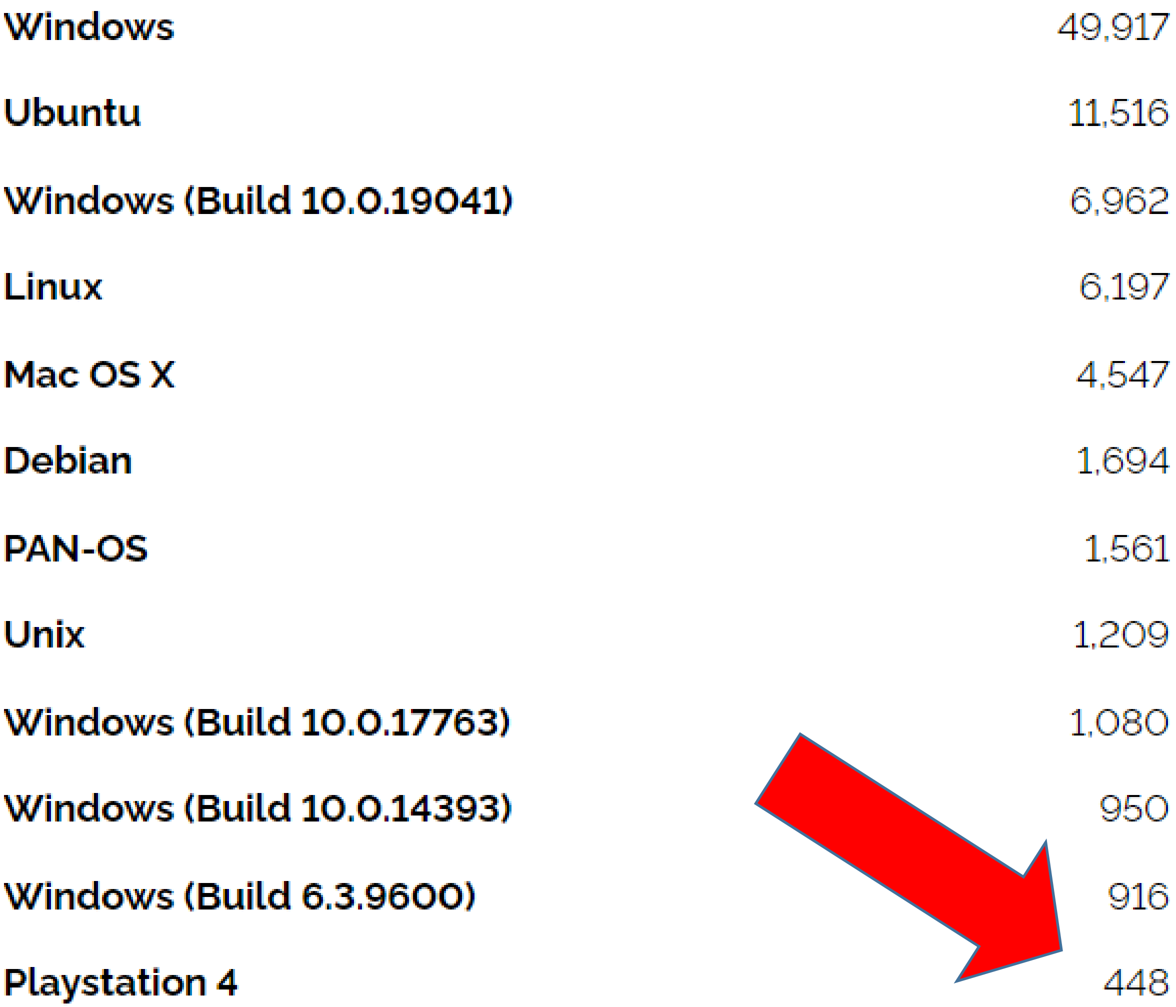
Cyber budget = $15 Billion

Cyber Budget = Gym Teacher

Problems in ED Data Systems

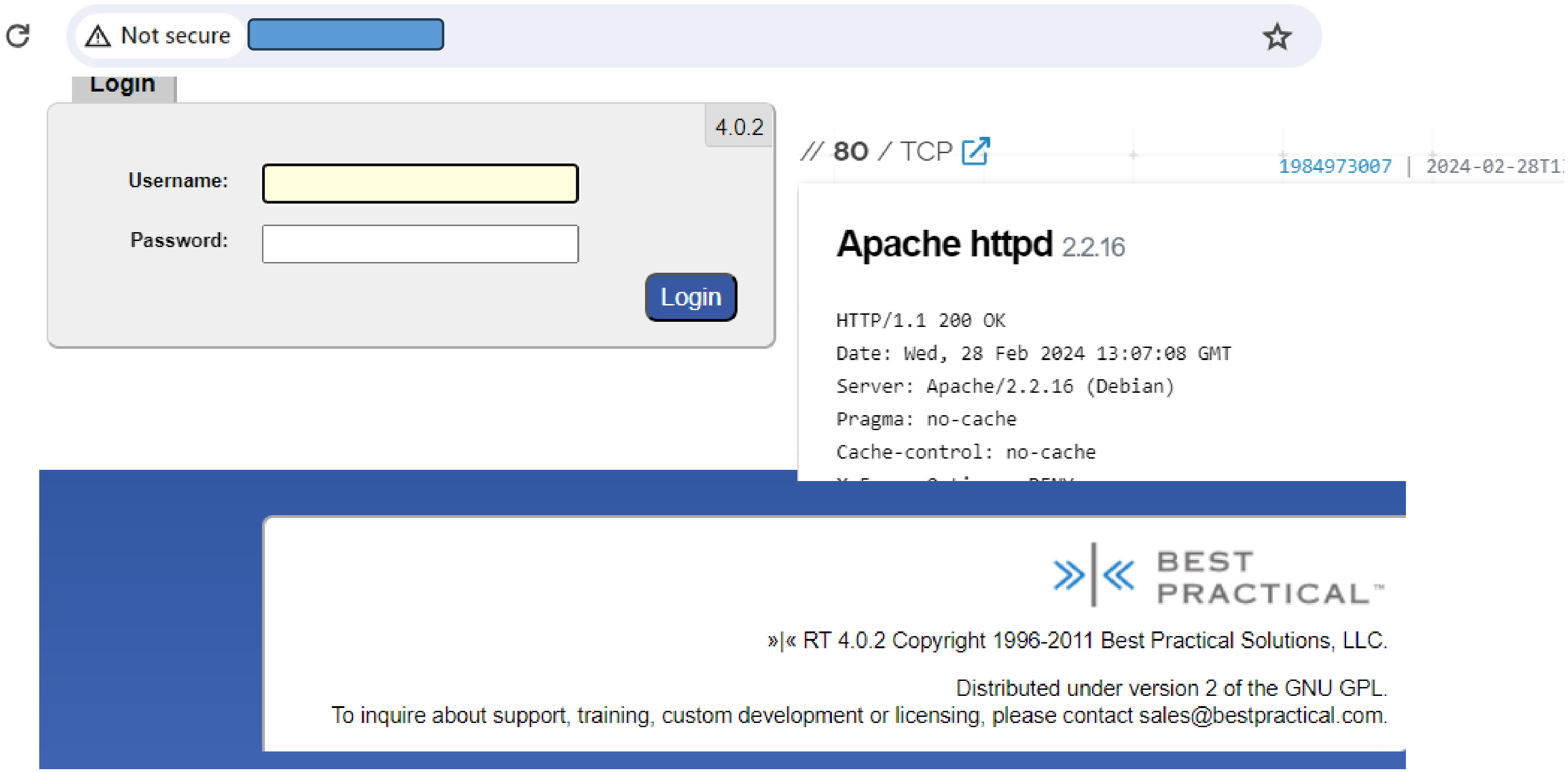
- A ***ton*** of old or unpatched software
- IoT devices in schools include:
  - *Server room cameras & sensors*
  - *School surveillance systems*
  - *Access card readers*
  - *Modems (UPnP hackable)*
  - *HVAC / Boilers*
- Hundreds of forgotten servers / computers
- Passwords
- Vendor / Cloud vulnerabilities
- People

Let’s Just Start Here



Windows	49,917
Ubuntu	11,516
Windows (Build 10.0.19041)	6,962
Linux	6,197
Mac OS X	4,547
Debian	1,694
PAN-OS	1,561
Unix	1,209
Windows (Build 10.0.17763)	1,080
Windows (Build 10.0.14393)	950
Windows (Build 6.3.9600)	916
Playstation 4	448

Legacy Software Sticks Out to Hackers



Not secure [redacted]

Login

4.0.2

Username:

Password:

// 80 / TCP

1984973007 | 2024-02-28T1

Apache httpd 2.2.16

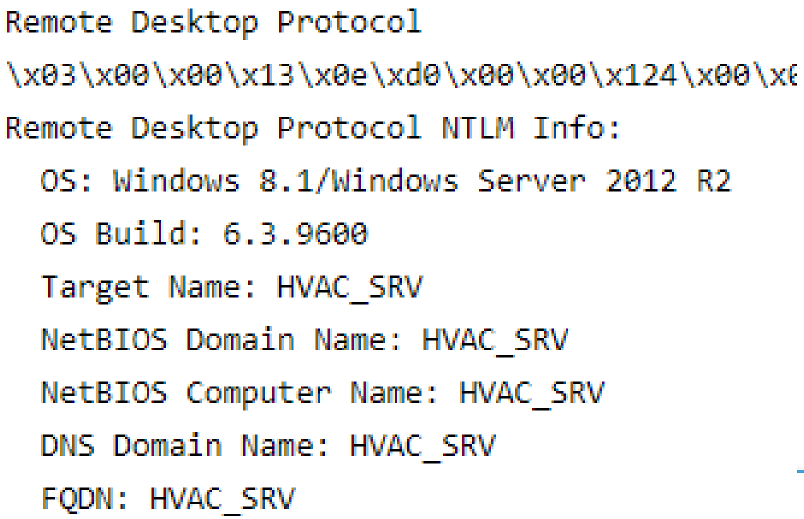
```
HTTP/1.1 200 OK
Date: Wed, 28 Feb 2024 13:07:08 GMT
Server: Apache/2.2.16 (Debian)
Pragma: no-cache
Cache-control: no-cache
```

BEST PRACTICAL™

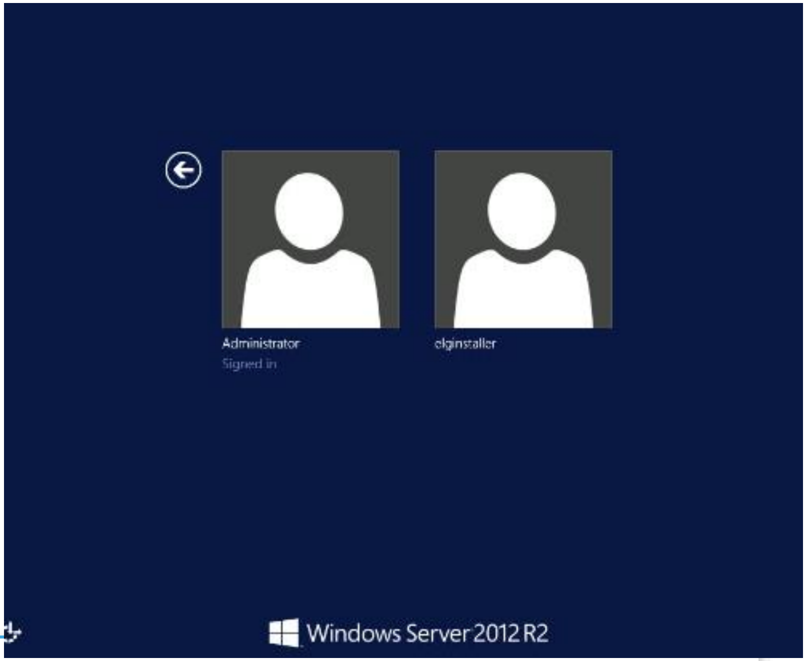
»|« RT 4.0.2 Copyright 1996-2011 Best Practical Solutions, LLC.

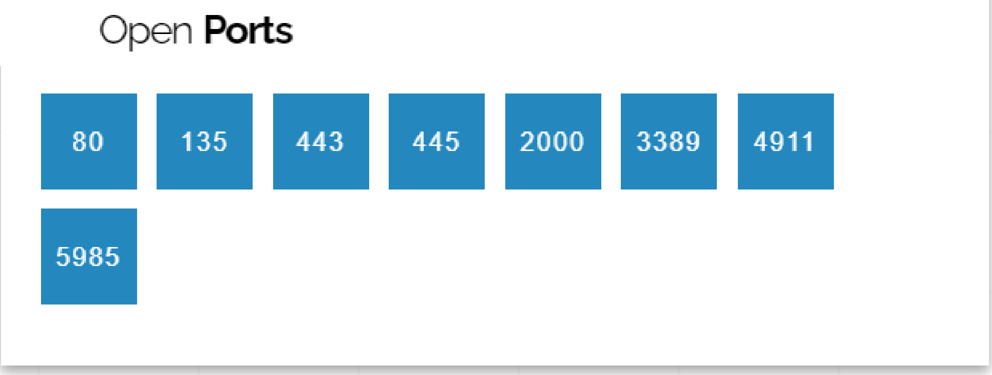
Distributed under version 2 of the GNU GPL.
To inquire about support, training, custom development or licensing, please contact sales@bestpractical.com.

HVAC is the new Hotness



```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x0
Remote Desktop Protocol NTLM Info:
  OS: Windows 8.1/Windows Server 2012 R2
  OS Build: 6.3.9600
  Target Name: HVAC_SRV
  NetBIOS Domain Name: HVAC_SRV
  NetBIOS Computer Name: HVAC_SRV
  DNS Domain Name: HVAC_SRV
  FQDN: HVAC_SRV
```

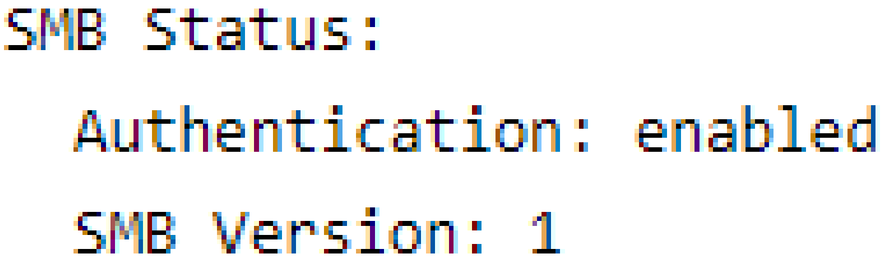




Open **Ports**

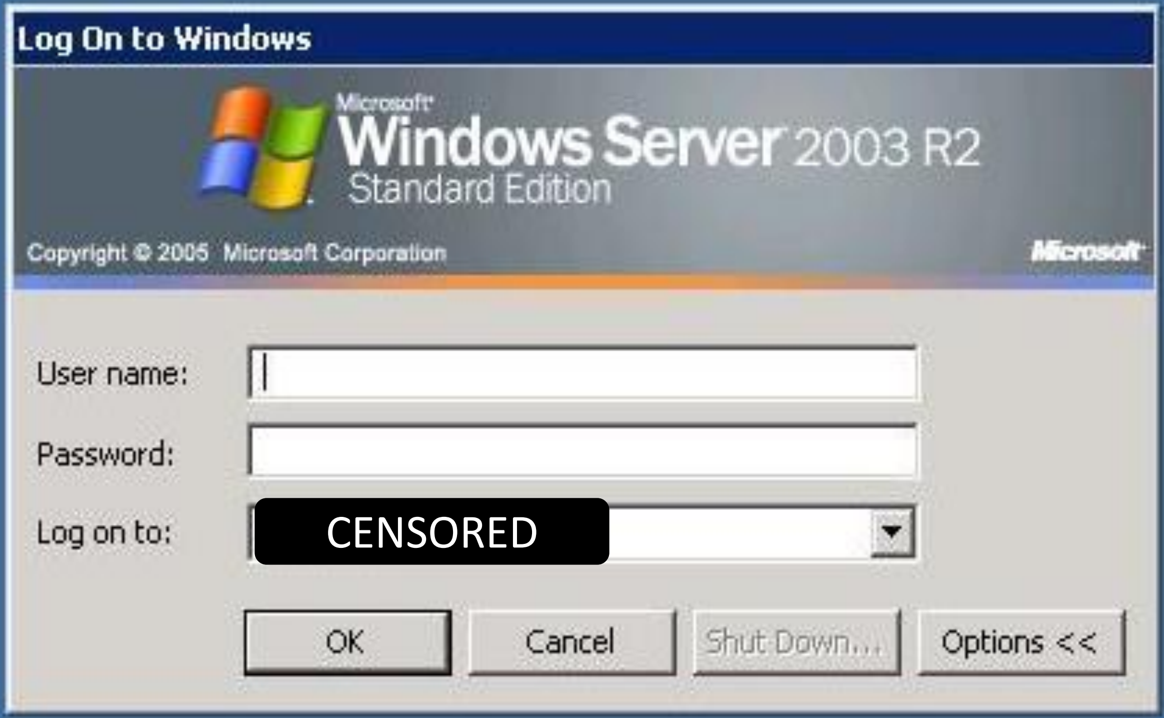
80 135 443 445 2000 3389 4911
5985

HVAC is the new Hotness

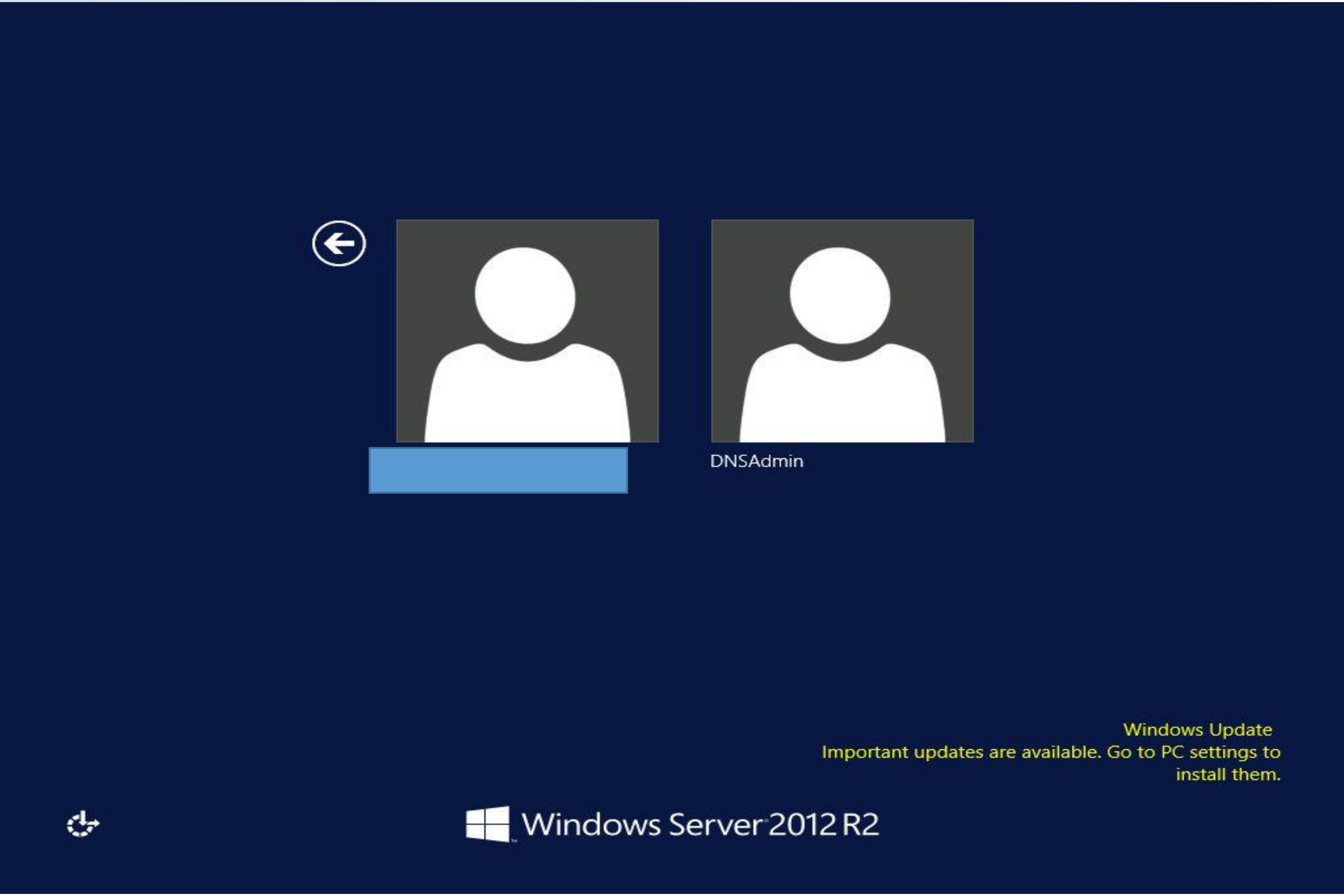


```
SMB Status:
  Authentication: enabled
  SMB Version: 1
```

Log On to Windows
Microsoft
Windows xp
Professional
Copyright © 1985-2001
Microsoft Corporation
Microsoft
User name:
Password:
OK
Cancel
Options >>



Log on to: CENSORED

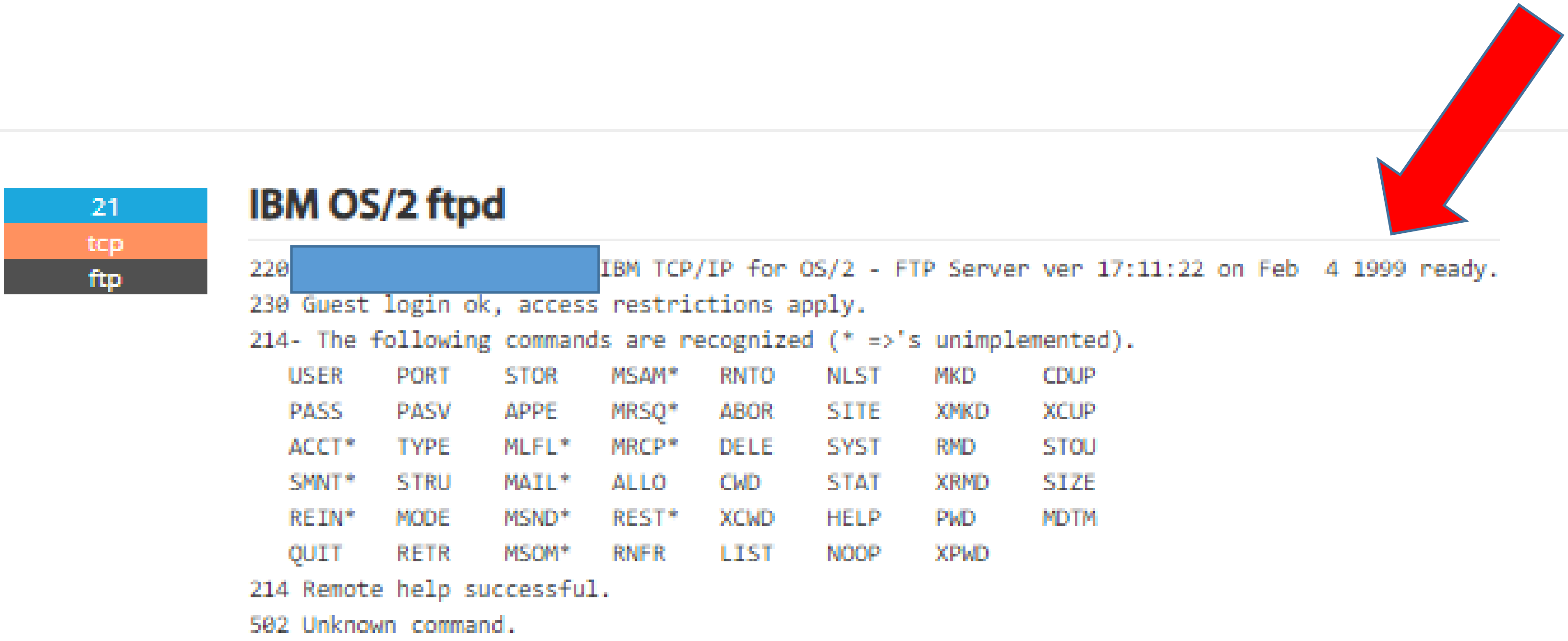


[redacted]

DNSAdmin

Windows Update
Important updates are available. Go to PC settings to install them.

The Reigning Champ!!



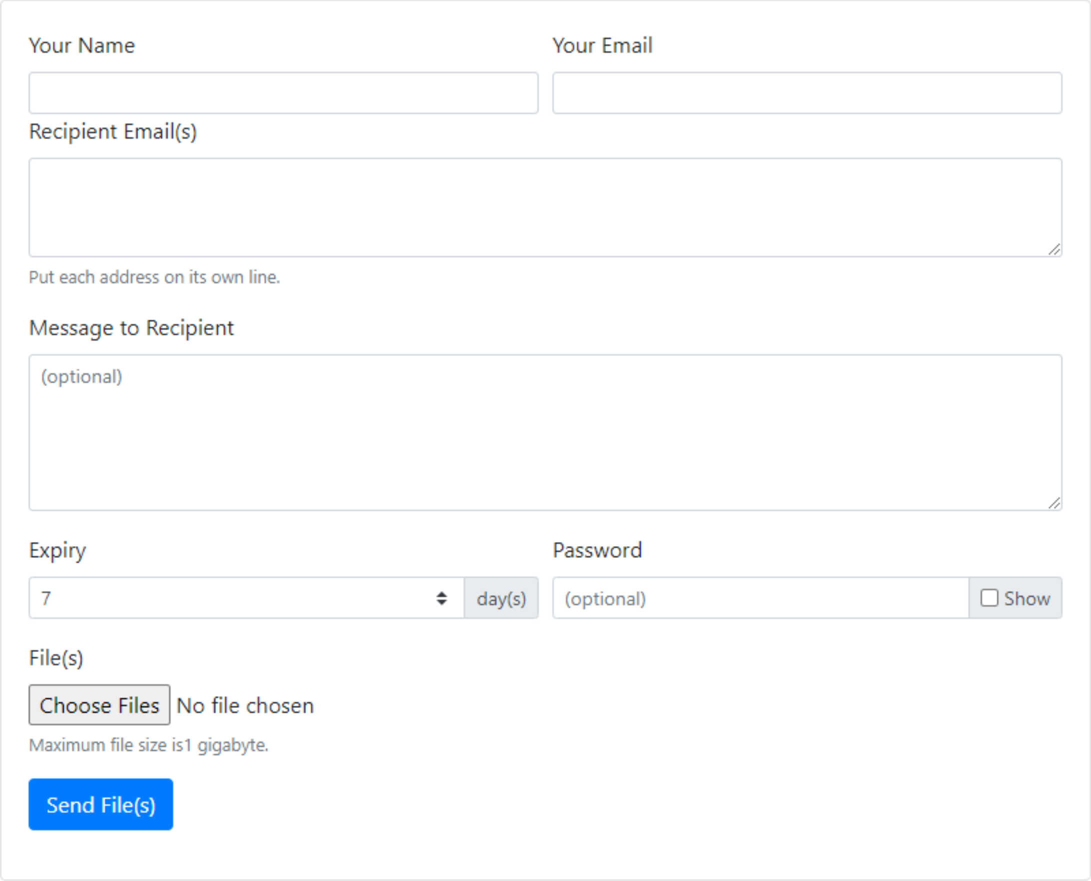
21
tcp
ftp

IBM OS/2 ftpd

```
220 [redacted] IBM TCP/IP for OS/2 - FTP Server ver 17:11:22 on Feb  4 1999 ready.
230 Guest login ok, access restrictions apply.
214- The following commands are recognized (* =>'s unimplemented).
   USER    PORT    STOR    MSAM*   RNTO    NLST    MKD     CDUP
   PASS    PASV    APPE    MRSQ*   ABOR    SITE    XMKD    XCUP
   ACCT*   TYPE    MLFL*   MRCP*   DELE    SYST    RMD     STOU
   SMNT*   STRU    MAIL*   ALLO    CWD     STAT    XRMD    SIZE
   REIN*   MODE    MSND*   REST*   XCWD    HELP    PWD     MDTM
   QUIT    RETR    MSOM*   RNFR    LIST    NOOP    XPWD
214 Remote help successful.
502 Unknown command.
```

Speaking of File Transfer

This is a public internet facing school web application that enables anyone on the internet to spoof any sender to send a file to any recipient with no apparent safety checks from a school domain.



Your Name

Your Email

Recipient Email(s)

Put each address on its own line.

Message to Recipient

(optional)

Expiry

7 day(s)

Password

(optional) □ Show

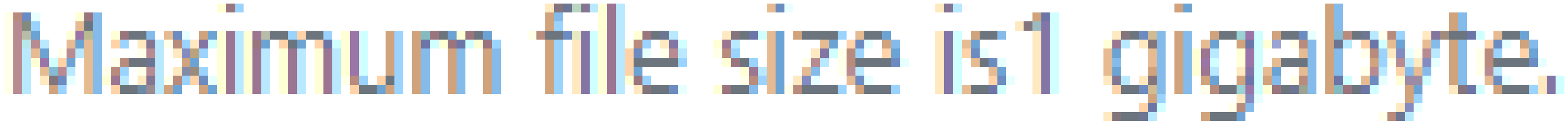
File(s)

Choose Files No file chosen

Maximum file size is1 gigabyte.

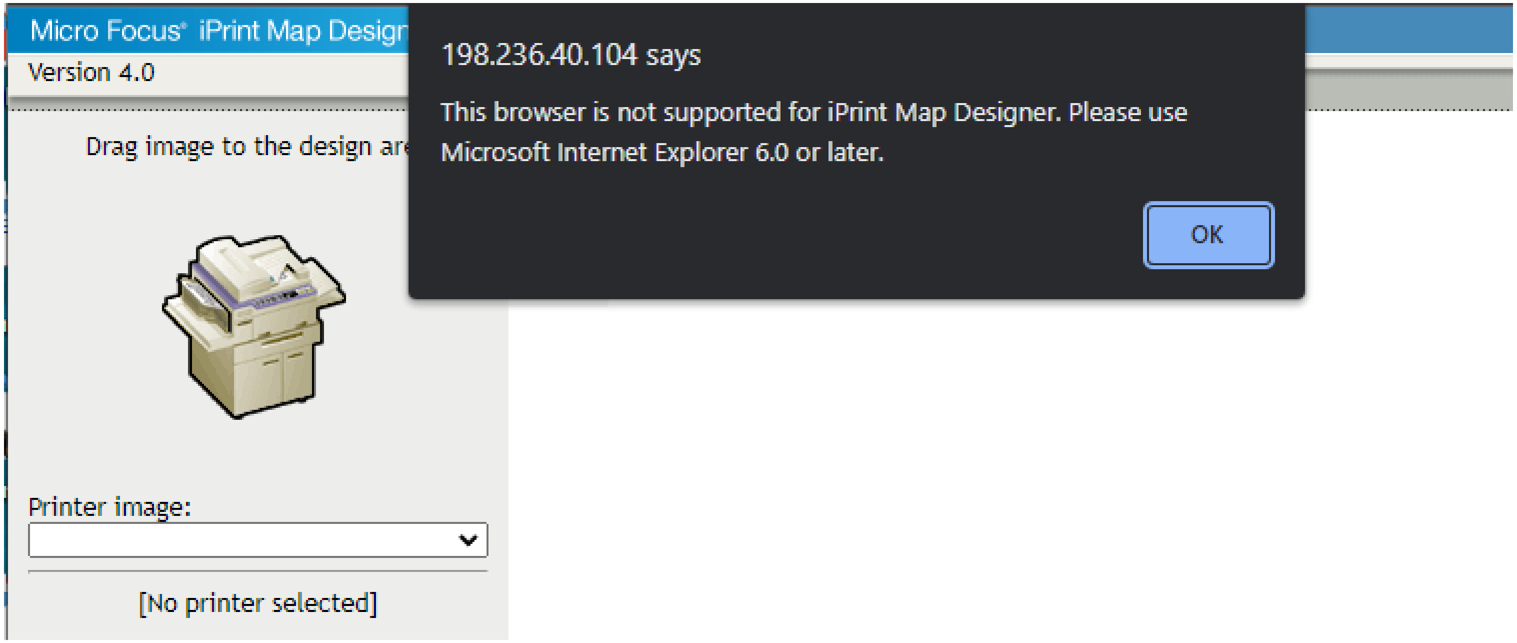
Send File(s)

Speaking of File Transfer



Maximum file size is1 gigabyte.

You know it's up to date when



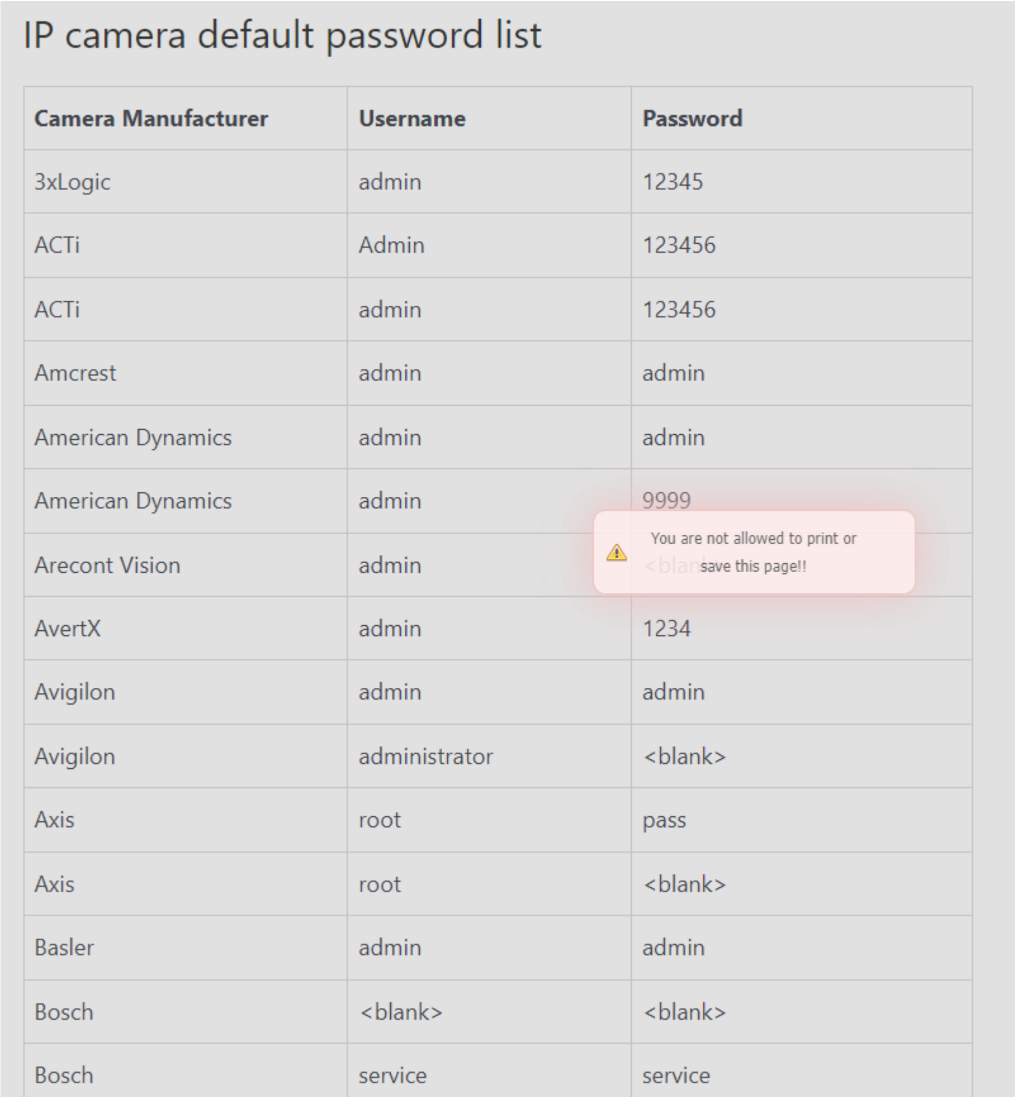
198.236.40.104 says

This browser is not supported for iPrint Map Designer. Please use Microsoft Internet Explorer 6.0 or later.

MH AV Anx Sun Apr 7 20:11:16 2019

Change Your Passwords…

Because these exist:

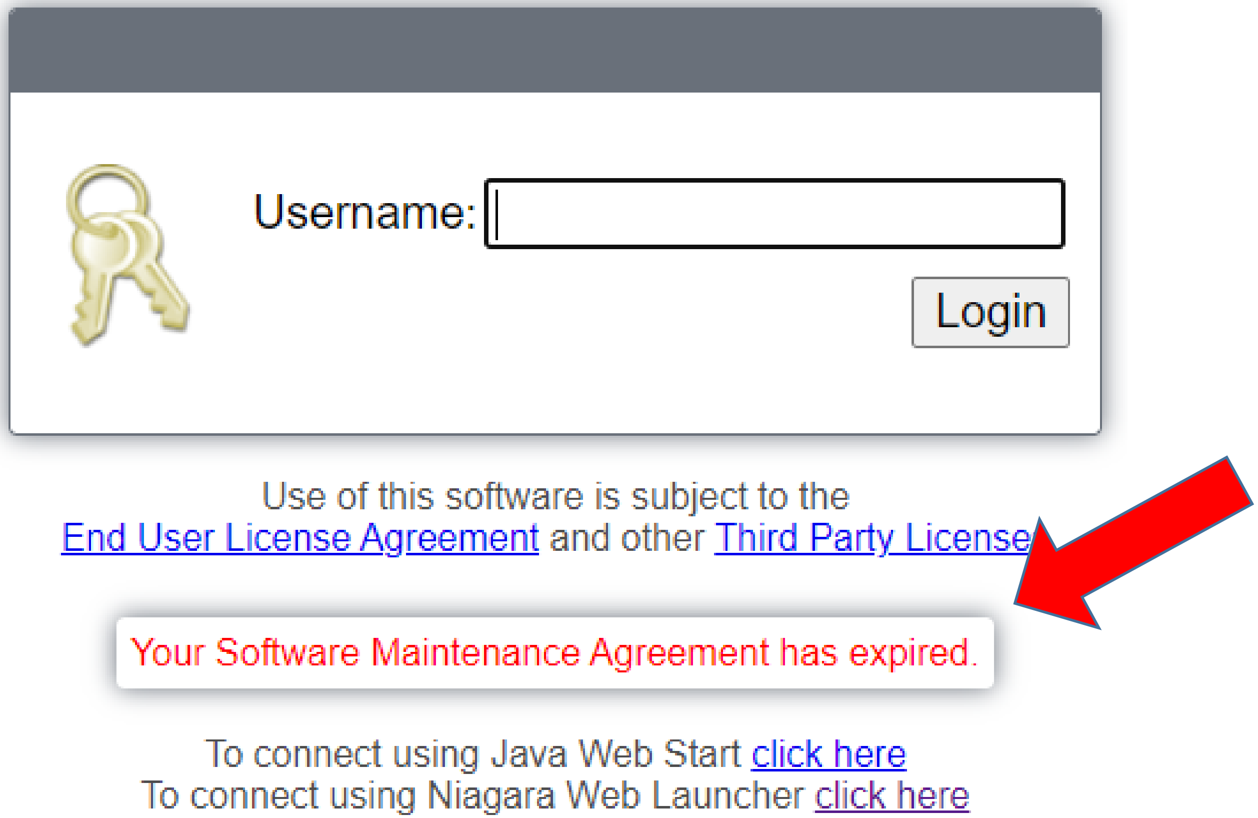


IP camera default password list

Camera Manufacturer	Username	Password
3xLogic	admin	12345
ACTi	Admin	123456
ACTi	admin	123456
Amcrest	admin	admin
American Dynamics	admin	admin
American Dynamics	admin	9999
Arecont Vision	admin	<blank>
AvertX	admin	1234
Avigilon	admin	admin
Avigilon	administrator	<blank>
Axis	root	pass
Axis	root	<blank>
Basler	admin	admin
Bosch	<blank>	<blank>
Bosch	service	service

⚠ You are not allowed to print or save this page!!

No More Patches?

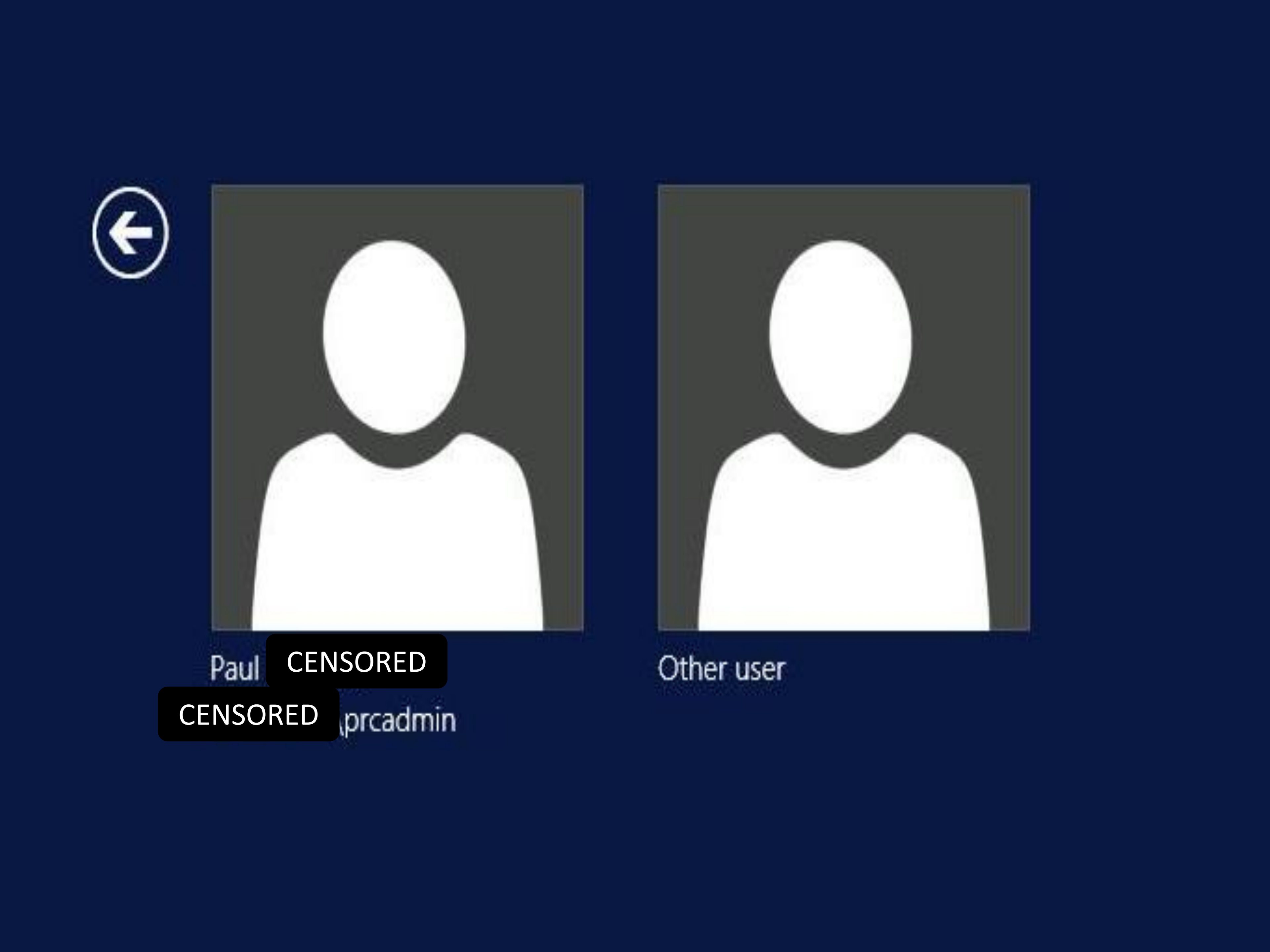


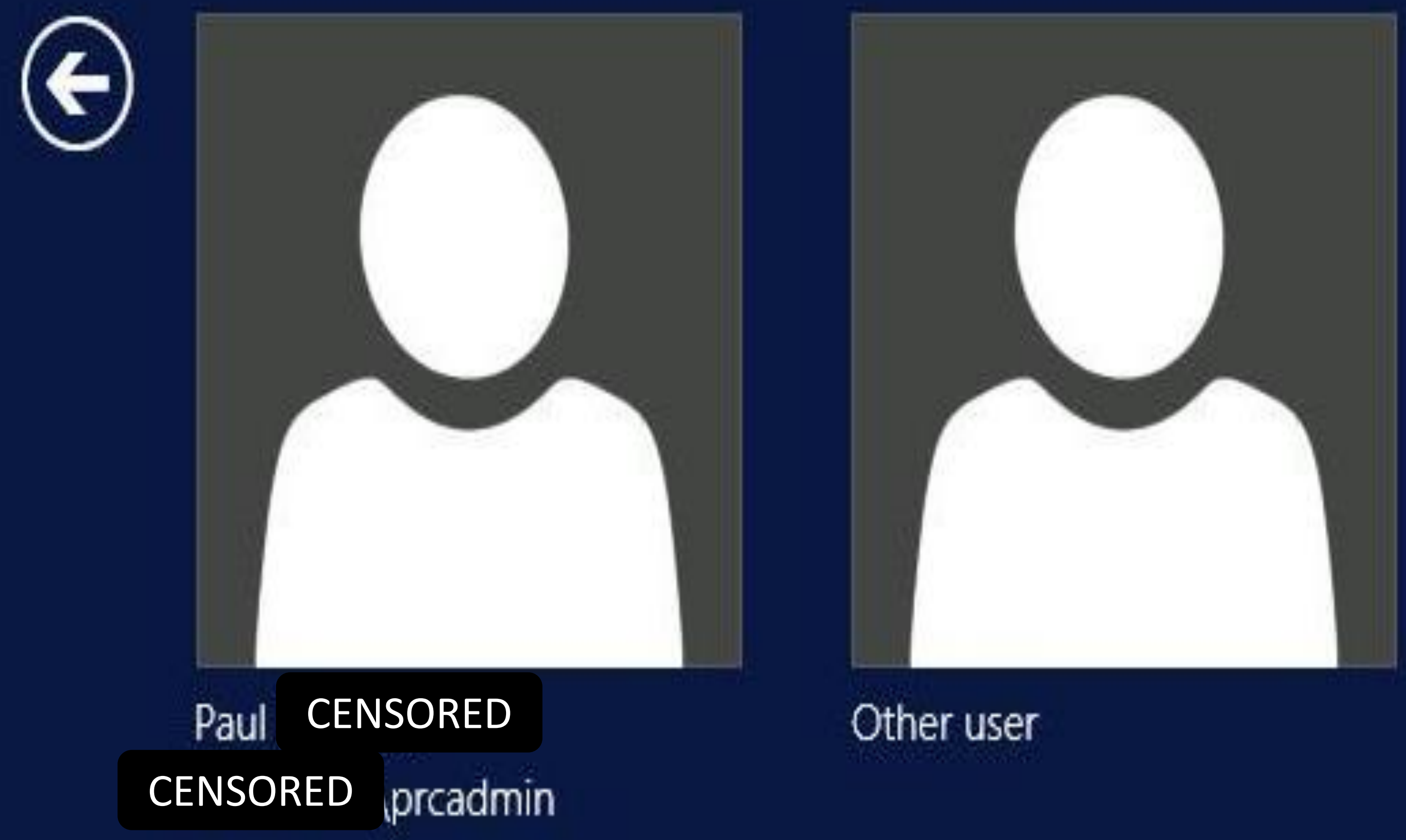
Use of this software is subject to the
End User License Agreement and other Third Party License

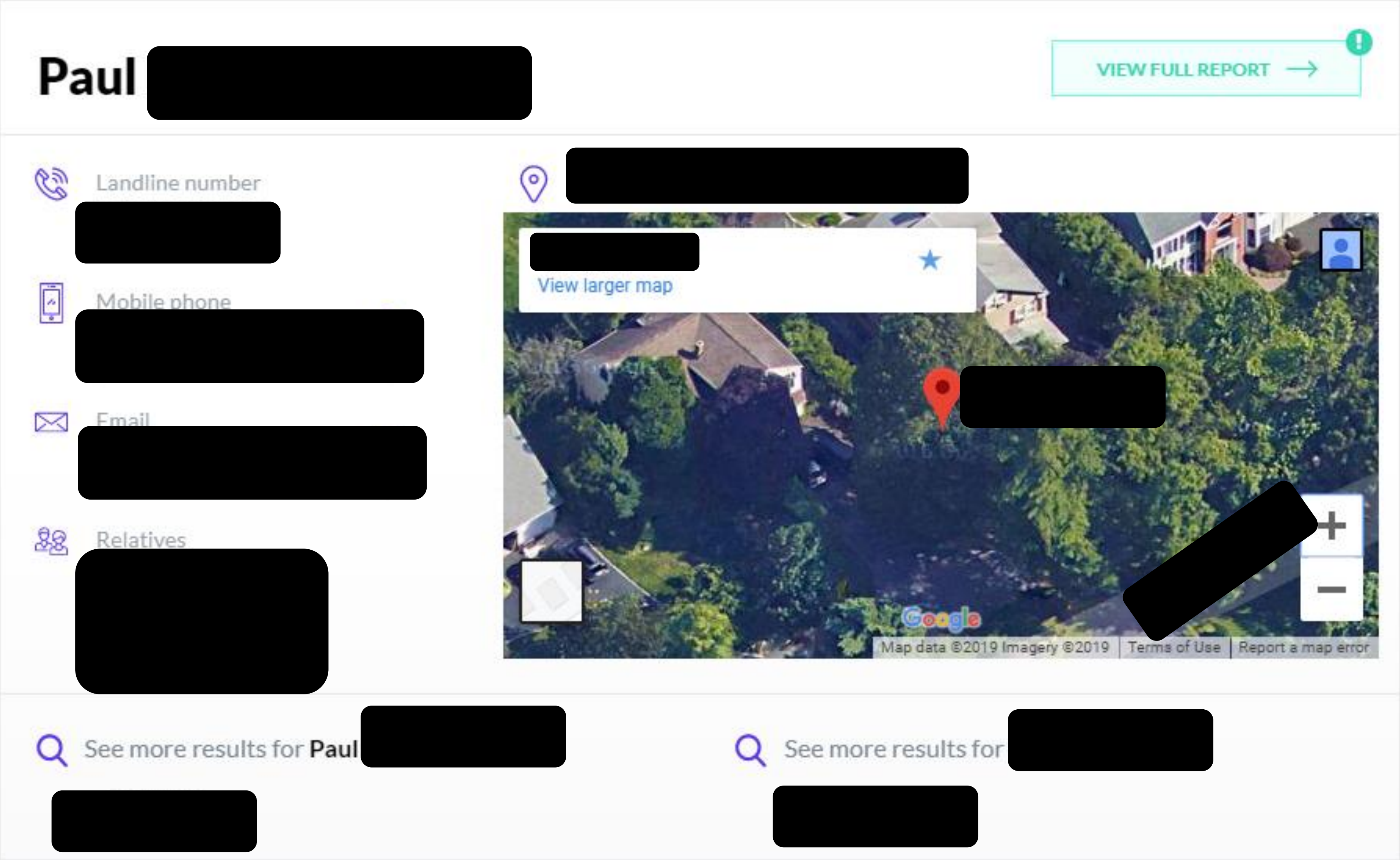
Your Software Maintenance Agreement has expired.

To connect using Java Web Start click here
To connect using Niagara Web Launcher click here

People – Your Employees are the Weakest Link


Paul CENSORED
CENSORED prcadmin
Other user


Paul CENSORED
CENSORED\prcadmin
Other user



Paul [redacted]

VIEW FULL REPORT →

Landline number
[redacted]

Mobile phone
[redacted]

Email
[redacted]

Relatives
[redacted]

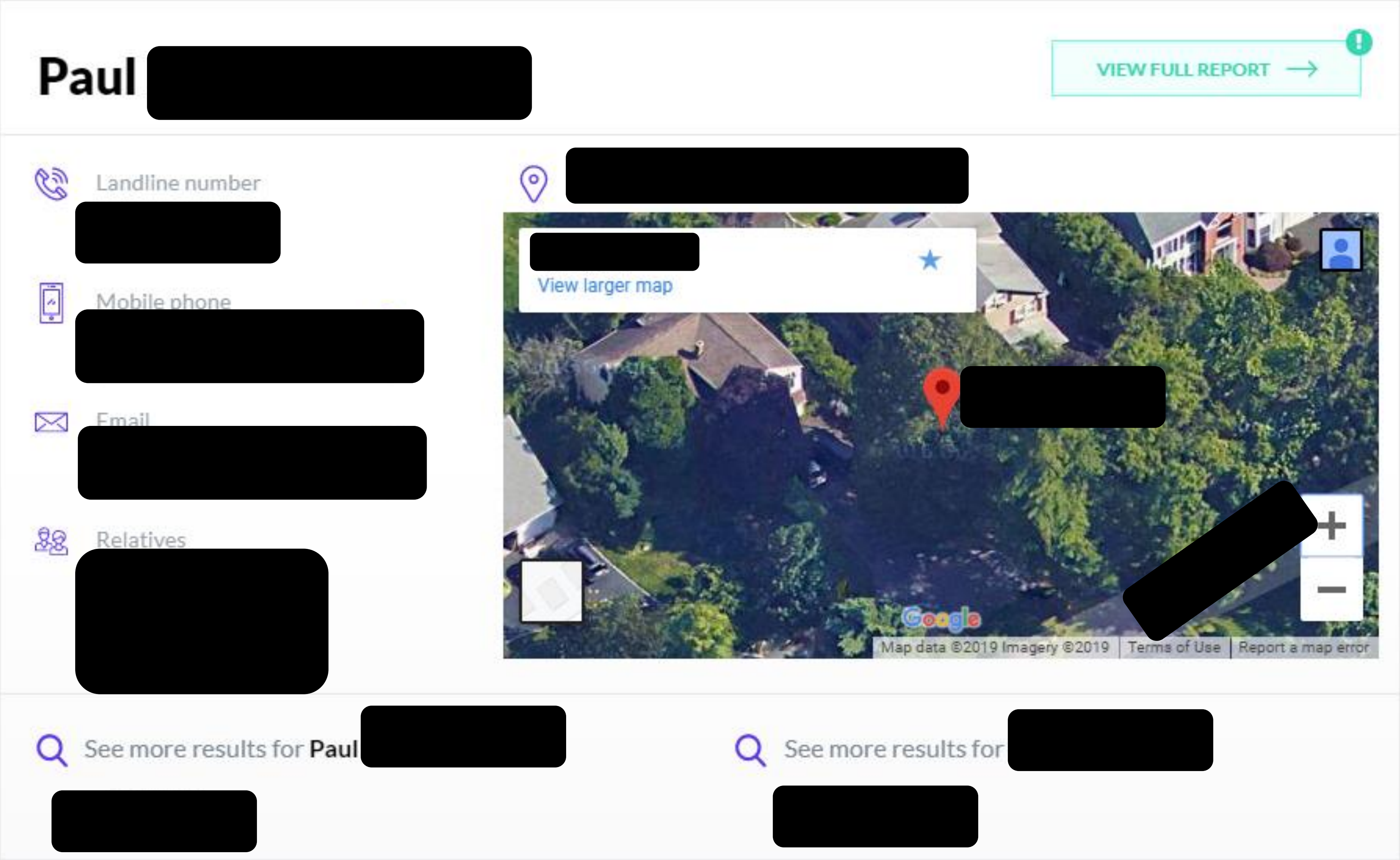
[redacted]

See more results for Paul [redacted]
[redacted]

See more results for [redacted]
[redacted]

CENSORED
Google

Linked in
textfiles.com_



Paul [redacted]

Landline number

[redacted]

Mobile phone

[redacted]

Email

[redacted]

Relatives

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

See more results for Paul [redacted]

[redacted]

See more results for [redacted]

[redacted]

CENSORED
Google

LinkedIn
textfiles.com_

How Attackers Exploit this Info

- Start high level and look at his papers, slides and emails to spot weaknesses in the enterprise
- Target with spear phishing / whaling attacks to phone, email, SMS
- Impersonation attacks against staff at the school
- Leverage friends & colleagues names to elicit action or shift focus to them
- Failing that, there's always blackmail, intimidation, coercion and threats

How Organizations are Vulnerable

Most phishing e-mails are easy to notice. Here are some things an attacker might do to gain access to your systems.

1. Locate Staff Directory (yes, it’s there)
2. Send phishing E-mail to targeted employees, infecting the unwary user
3. Locate and exfiltrate data
4. Profit!

Isn’t this someone else’s problem?

- **Most breaches start with social engineering**
- **Attackers target <u>YOU</u>, not the technology first**
- **Most successful large breaches use stolen credentials!!!!!!!**

Security Tips for Users

Enterprise controls only extend to the network boundary. Users take their devices on the road, to the airport and the local coffee shop.

Here are what users can do to protect themselves when away from the office:

- ***Be aware of common threats***
- ***Take concrete steps to reduce risk***

What to do - Individually

- Use encryption. SSL/TLS, VPN, Full-disk, file level.
- Verify website are secure by visually checking.
- Treat all WiFi as untrusted WiFi.
- Use strong passwords.
- Multi-factor authentication is your friend
- Check links in emails and documents before clicking through them.
- Never plug in a strange flash drive.
- Set a screen lock.
- Patch and update regularly, especially for third party applications.

Data Security is a Shared Responsibility

IT

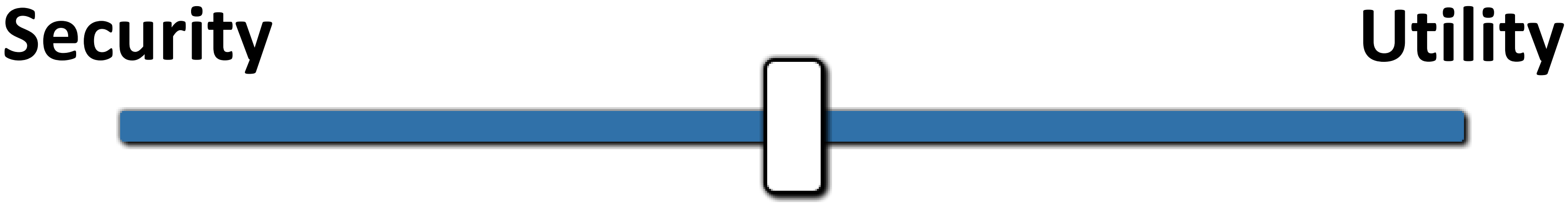
- Vulnerability Mgmt
- Account Mgmt
- Boundary Control
- Performance Metrics

Shared

- Privacy & Security Training
- Incident Response
- Risk Management
- Data Accountability

Tailor Data Security to Your Business

Do not forget that the purpose of the systems is to enable the business of educating children!



Security

Utility

Data Security

Bare Bones Must Haves:

For a Strong Data Security Foundation

- Privacy & IT security Training annually
- Agile Vulnerability Management
- Formalized Risk Management Processes
- Incident Response Plan & Team
- Strong Account Management
- Adopt Common Data & System Standards
- Enforcement of Standards

Most Importantly

- Leadership buy in

Incident Response: What’s Inside the Box?

Key phases typically include:

1. **Preparation**: Defining the response team, roles and responsibilities, developing communication plans, and resourcing
2. **Identification**: Detecting and determining the nature of the incident.
3. **Containment**: Containing the incident, mitigating further damage
4. **Eradication**: This involves removing the threat from the affected systems
5. **Recovery**: Restoring and returning systems and networks to normal operations
6. **Lessons Learned**: Post-mortem analysis and lessons learned for process improvement

Step #1: Have a Plan

Failure to plan is planning to Fail…

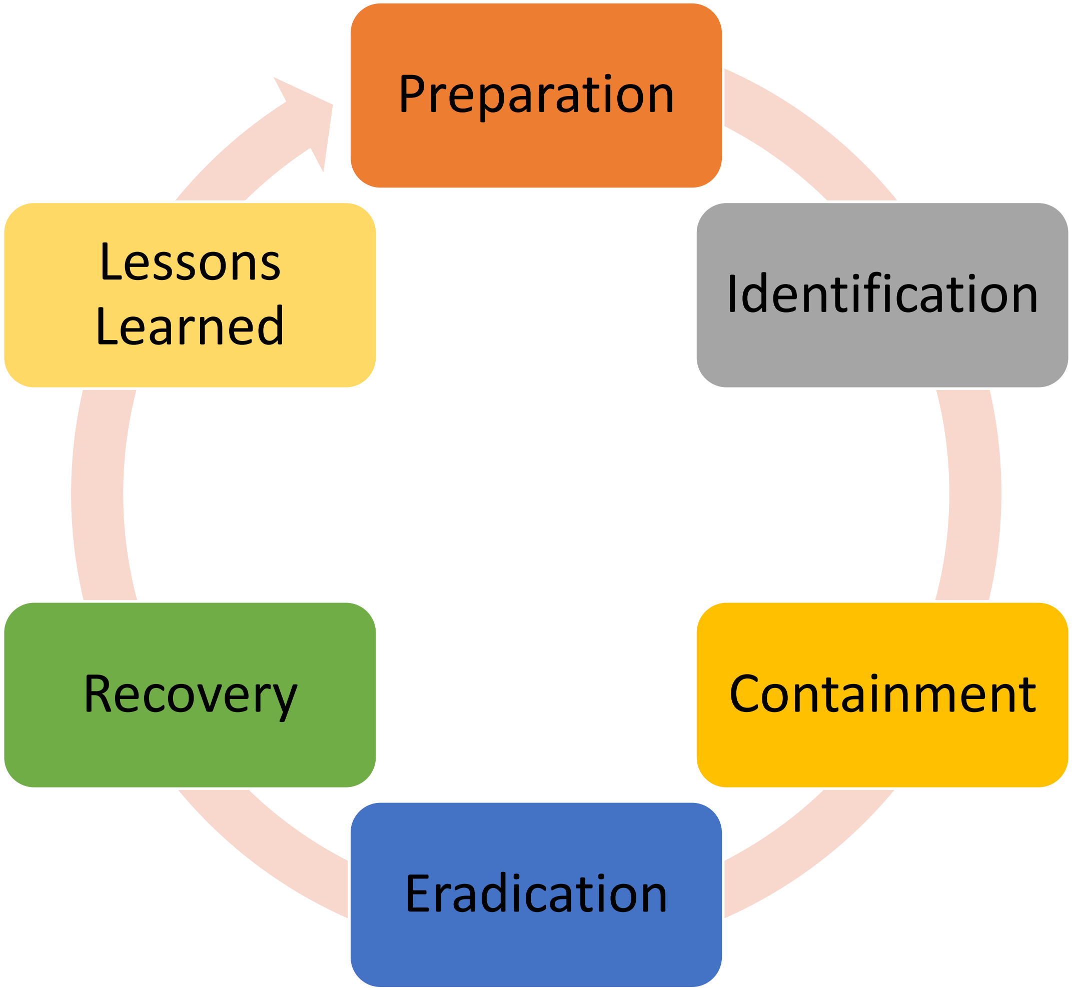
You Need an Incident Response Plan

Incident Response Plans

"An Incident Response Plan is a written document, formally approved by the senior leadership team, that helps your organization before, during, and after a confirmed or suspected security incident." -CISA

- *Defines the Purpose / Mission*
- *Identifies Roles & Responsibilities*
- *Sets organizational priorities*
- *Determines response thresholds*
- *Outlines response processes*
- *Creates standards for documentation & metrics*
- *Establishes compliance & review timelines*

Putting a Plan Together



Preparation

Identification

Containment

Eradication

Recovery

Lessons Learned

Putting a Plan Together

- Determine the "Musts"
- Define your Stakeholders
- Obtain leadership buy-in
- Understand what you have
- Evaluate the threat
- Perform a risk-assessment

Incident Response Teams

There are two key success factors to good Incident Response Team performance.

The right Team

&

Somebody in-charge

Incident Response Team

Incident Response Teams are groups tasked with the response, management, and recovery of security and privacy incidents.

CORE

- Leadership
- Legal
- Communications / PA
- IT

AD-HOC

- Vendors / Partners
- Law Enforcement
- Facilities
- State Agencies

Incident Response Team Responsibilities

- Assess, analyze, and manage incidents from initial reporting to out-brief
- Speed recovery, ensure threat data flow, contain the incident
- Coordinate with stakeholders, decisionmakers, regulatory bodies, and communicate
- Documentation & reporting of response actions
- Post-incident analysis, prevention, education, and training

Who’s in Charge Here?
The Role of the Incident Manager

Acts as the coordinator and focal point for the response efforts

Key Responsibilities Include:

- Incident Coordination & Mgmt
- Communication
- Decision Making
- Strategy & Planning
- Resource Allocation
- Post-Incident Review
- Compliance Considerations
- Process Improvement
- Training & Awareness

Let’s Talk IR Secret Sauce

Secrets to *less Painful Incident Response:

- Not Owned by IT
- **Includes Legal Counsel & Public Affairs**
- Starts with Validation
- Continuous review & testing
- Incorporates lessons learned

Leadership Involvement

- Formal policy & plan
- Publicized and socialized throughout the organization
- Supported by reporting & feedback mechanisms
- Policy should assign roles and responsibilities, including leadership presence on IRT
- Absolutely NOT just an IT thing!

Legal Eagles

Legal Counsel is a huge benefit in incident response. This could be your local counsel, outside counsel *(or even cyber-insurance company).*

- Often confusing legal requirements
- Need to protect organizational interests
- Interfacing with Law Enforcement & State entities

Communications is KEY

Think about including Public Affairs / Communications representatives in your IRT. Message is the often the hardest part of a response

- Ransomware & DDoS require some ‘splaining
- Need concise, clear, consistent messaging both internally and externally
- Frees up critical response resources
- Consistency of messaging conveys reassurance that the response is under control

Would you like to play a game?

Threats evolve, so should your Incident Response plan!

- *Periodic risk assessments*
- *Annual IR exercise*
- *Involve third-parties, vendors, and partners*
- *Use as an opportunity to talk to law enforcement, cyber-insurance reps, contractors, etc.*

Tabletop Exercises

Simulated incident response based on carefully selected scenarios, where the IRT sits down and walks through a response.

- Build IRT cohesiveness and confidence
- Establish lines of communication
- Identify problem areas and streamline the IRP
- Ensure process and plans are extensible to the widest spectrum of incidents

Data Breach Resources

Downloadable Data Breach Training Kits

https://studentprivacy.ed.gov/resources/data-breach-scenario-trainings

New Expansion Pack Available!

Feedback Loops

"The most neglected part of the incident response plan is the part where you remember all the mistakes you made and fix them for next time"

-**Me**

Feedback Loops

Every organization should document their process and capture important data for process improvement:

- *What worked well?*
- *What didn't work at all?*
- *Did we miss something?*
- *What can we do better?*

Final Food for Thought

- You should have an incident response plan in place and train to it
- Data privacy & security awareness training for all employees, as well as contractors, researchers, and other 3rd parties
- Clearly understand the legal requirements for compliance with all applicable federal, state and local laws
- Consider calling PTAC, we can help!!!

Data Breach Scenario Exercise

Background

You work for the Little Bend High School, which is a school of just over 700 students in a small suburb of a major metropolitan area.

In 2021, your high school fell victim to a ransomware attack that took down your school for a week and lead to a leakage of student data.

Background

Your school is currently part of a statewide effort to address school safety concerns through a program which attempts to identify students who are at risk for violence or self harm in order to provide resources and counselling before a potential issue occurs.

The state has provided grants to schools to help them conduct threat assessments and provide funding for early interventions and student support.

Background

Over the last few weeks, the school has worked with local authorities, vendors, and third-party contractors to review school records, public social media posts, and law enforcement records to identify students who may be in need of help.

The team has identified three students who meet the established criteria. Juan (junior), Brandon (senior), and Jennifer (freshman) are all students in your school who have red flags for a potential for violence or self-harm.

Background

Reports from the school safety task force indicate that Juan and Brandon are loners and have had a history of aggressive acts outside of school. Both have few friends and some discipline issues, as they have been involved in altercations at school.

Jennifer has been identified as being at risk for self-harm because of a clinical diagnosis of depression, coupled with social media posts about being alone and wanting to run away.

Background

- The team compiles their findings into a draft report and makes it available to school leadership and the lead counselor.
- The draft report needs to be reviewed and approved before any actions are taken and parents notified.

Background

Several days later you receive complaints from the parents of the students identified in the report. They say that your poor security practices lead to another data breach.

They claim that their children are being bullied and harassed online by their peers. Parents are threatening to sue the school, claiming that their children have been victimized by this disclosure.

What Now?

Clearly the information from the report has not remained confidential. What steps would you take to begin to address this situation?

Do you think that a data breach has occurred?

Consider:

- What is a data breach?
- Do you know enough to make any assertions at this point?
- What are your first steps to respond?

Where are we? Let's recap.

- Draft school safety assessment has been completed.
- Shortly thereafter, some students identified in the report begin being bullied by other students.
- Parents are livid that their children were included in the report and that the information got out.

Which is Best?

A. IT Director calls the safety task force and demands answers

B. Break out your incident response plan and convene the IRT to begin working the issue.

C. Panic, delegate a bunch of duties, then upload your resume to a bunch of online job sites

But Wait… You Have a Plan!

Because you attended the PTAC session on incident response last year, you have an excellent plan to deal with these types of issues.

The Event Evolves

You spin up your incident response team and begin to investigate how the information was made public. The report is saved on a secure file share, but the report was delivered via email to the principal and counselor.

Your IT staff, still feeling the organizational trauma of the breach in 2021, begin examining the school network for signs of compromise.

The Event Evolves

The press is continuing to hammer at the school and the state government for what it calls "intrusive, Orwellian surveillance of students." The public is demanding answers as to what is going on at the school and how this information was made public.

Furthermore, since the data has been released, several parent groups are calling for the immediate dismissal of your IT Director following the second breach in two years.

Let's stop and think

Things to consider:

- Is this information covered by FERPA? Is this a FERPA violation or a data breach?
- Does the type of data impact whether it is a breach?
- What role do state laws play?
- Who should be involved in your response activities?

The Event Evolves

The principal was out of the office when the report was emailed, presenting at a State education conference. The school counselor recalls that he saved the attachment to his network drive and took a paper copy home to read after hours. He produces the paper copy complete with coffee stains and interspersed with his handwritten notes.

The principal read the document on her iPad at the conference over lunch. She sent a couple of emails to the counselor about her concerns about the report, suggesting redaction and questions about the recommendations in the draft report.

What Now?

We know who received the information, but there is no real indication at this point of a breach? What, if anything, do you tell the public at this point? Is this a Data Breach or a FERPA violation? Both?

Consider:

- What are you going to tell the press / public?
- What about FERPA? Was this part of the education record?
- Where will you take the investigation now?

Let’s Discuss

- Two people at the school, the principal and the counselor got the email with the report
- The counselor saved it to his network folder and the principal viewed it online.
- The press and irate parents are breathing down your neck, and there are no immediate indicators of nefarious activity.

IT Weighs In

IT completes it check of the logs for the email and file servers. There are no indications of unauthorized activity or access to the email accounts or files on the shared drive. The e-mails in question were sent to the correct recipients and were even encrypted in transit. The only access has been from school owned computers. Access to the file share was locked down, so only a select few school officials could access the report.

The principal had a call to the IT service desk about a problem with the wireless network, but it was resolved as a password issue.

Finally, a Break

The local news has printed a redacted image of the report on their website. However, they are unwilling to provide information on where they obtained the material beyond saying that they received it from an unnamed confidential source. You question all employees, and no one admits to leaking the document.

Finally, a Break

One of your school office staff recognize that the image in the paper shows a series of lines running down the printed page. The staff member shows you a document that they printed from the main office printer / copier just now which has the same pattern of lines.

What Now?

So, the news says they received a printed copy, but they refuse to give up their source. An observant staffer notices a pattern that indicates that the leaked doc was printed at the main office. What do you do now? Does this indicate malicious activity? Do you update the public on this information?

Consider:

- How does this affect the investigation? Is this a criminal act?
- Do you call the authorities? If so, who?
- What steps will you take now? What can you do to mitigate the damage to the victims?

Let’s Review

- The press has released a redacted copy of the draft report on their website
- Somebody printed the document the press has from the main office printer.
- The staff all deny any knowledge of the leak.

Wrapping Up

When you check the logs from the main office printer you find that the counselor attempted to print the report, but that there was an error because there was no paper left in the machine.

The counselor explains that he remembers the attempt to print but just figured that the printer was broken and printed from another printer on the other side of the office.

Wrapping Up

Meanwhile, in an effort to reduce the harm to the victims, you bring in the students who have been bullying the victims in for a talk. One of them says that another student named Terrance showed them the report and says that he found it laying on the printer in the office.

Terrance is a sophomore who is often in the office as an active member of the student council. When you ask him about the incident, he says that he picked up a stack of fliers from the printer and found the document. He viewed it his civic duty to let the public know about how potentially dangerous students were being allowed to continue to attend school. He provided the document to the local news station through email via their tip line.

Wrapping Up

So, it appears that a printer error triggered this whole incident. The activist student picked up the document by accident and provided it to the news believing himself to be a whistleblower.

Where does this leave the school?

- Is this a data breach?
- Who do you need to call / contact?
- Was a crime committed?
- How do you resolve this issue?
- What about the victims?

Lessons Learned From Incident Response

- Oftentimes the full extent of the issue is not known at the beginning of the incident
- Things can, and often do, get worse
- With student data involved – emotions tend to be heightened – parents have questions and want answers
- Incident response is not an IT problem – it is an everyone problem

Questions?

CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center

☎ (855) 249-3072
(202) 260-3887

✉ privacyTA@ed.gov

💻 https://studentprivacy.ed.gov

📠 (855) 249-3073