Cybersecurity Concerns for Facilities

MSBO Annual Meeting

Merri Lynn Colligan, Washtenaw ISD
David Larson, Livingston ESA
Matt McMahon, Gratiot-Isabella RESD
Joel Phillips, Newaygo County RESA

Introductions & Objectives

- Learn how common systems can be compromised
- Understand how best to protect against intrusion
- Hear case studies of what can happen when systems are attacked
- Things to discuss with your techs & vendors

Reasons for Concern

- Potential Liability
- Legal Requirements
- District Reputation
- Professional Reputation
- Staff and Student Records
- Monetary losses
- Loss of data (Key records, HVAC, logs, etc)
- Disruption of Services - virtual can affect physical

Data Breaches in Education

How

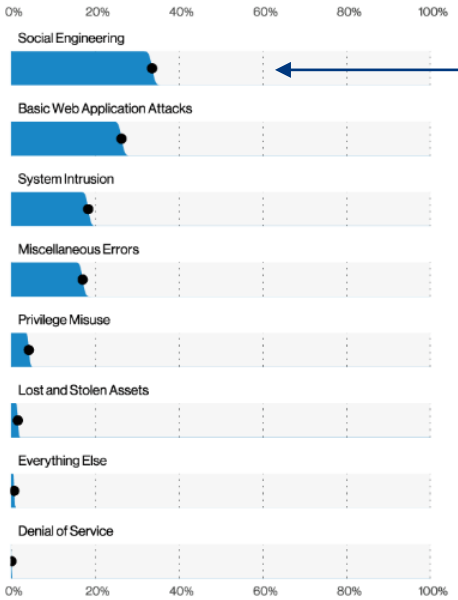


Figure 5. Patterns in breaches (n=5,275)

People

Who

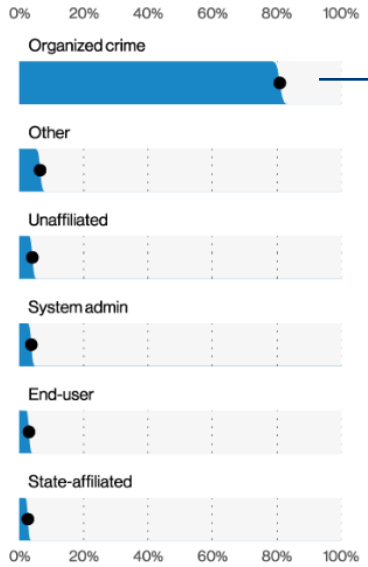


Figure 16. Top threat actor varieties in breaches (n=2,277)

Internet

What

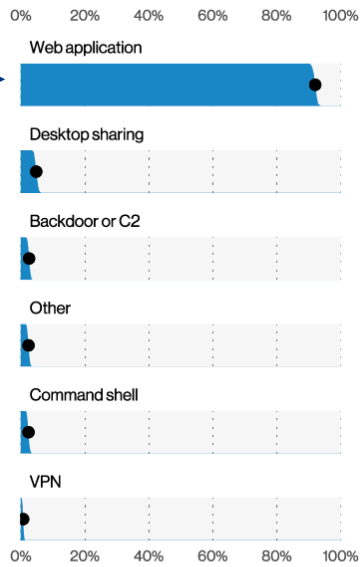


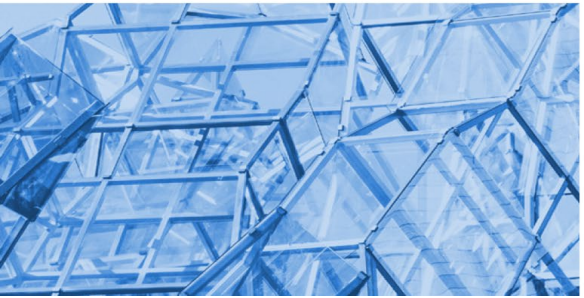
Figure 26. Top Hacking vectors in breaches (n=1,610)

Verizon 2021 Data Breach Investigations Report

Attackers generally follow these steps to compromise an organization - Any entry point will be used.

http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

Essential Cybersecurity Practices for K12



MISecure.org

Produced by METL,
a workgroup of MAISA

Created for Michigan Schools

By Michigan K-12 technology experts

CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

CIS® Center for Internet Security®

**CIS V8 Controls have recently been reduced to 18.*

Basic CIS Controls

1. Inventory and Control of **Hardware** Assets
    a. *What physical equipment do you have*

1. Inventory and Control of **Software** Assets
    a. *What software is running on your hardware*

1. Continuous **Vulnerability** Management
    a. *Who is patching/updating*

Basic CIS Controls

4. Controlled Use of **Administrative Privileges**

   a. Who has the master keys

5. Secure **Configuration** for Hardware and Software

   a. Change the default passwords. No direct Internet access (behind VPN, remote mgt tool)

6. Maintenance, Monitoring and Analysis of **Audit Logs**

   a. How far back can you tell who accessed what and when

2020-10 - MSBO - Cy | Cyber Security Applie | 20200908 Agenda - G | Extensions - Screen R | http net: | American Auto-Matrix | New Tab

shodan.io/search?query=http+net%3A%2F24"

Apps | Work | Home | News | Munis | Udemy | Data Breach | Other bookmarks

Shodan | Developers | Monitor | View All... | Show API Key | Try out the new beta website! | Help Center

SHODAN | http net: | Explore | Downloads | Reports | Pricing | Enterprise Access | My Account

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

21

TOP COUNTRIES

United States	21

TOP SERVICES

HTTP	6
HTTPS	4
8001	3
HTTP (8080)	3
HTTPS (8443)	3

TOP ORGANIZATIONS

Merit Network	21

TOP PRODUCTS

Apache Tomcat/Coyote JSP engine	8
Squid http proxy	7
Microsoft IIS httpd	2
lighttpd	2
Mongrel httpd	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Merit Network
Added on 2020-09-03 13:20:42 GMT
United States, Clare

```
HTTP/1.1 200 OK
X-Powered-By: PHP/5.6.30
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 03 Sep 2020 13:20:40 GMT
Server: lighttpd/1.4.32
```

American Auto-Matrix

Merit Network
Added on 2020-09-03 00:06:24 GMT
United States, Saint Johns

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
X-Powered-By: PHP/4.4.8
Content-type: text/html
Date: Thu, 03 Sep 2020 00:06:12 GMT
Server: lighttpd/1.4.18
```

Student and Parent Sign In

Merit Network
Added on 2020-09-07 07:39:13 GMT
United States, Clare
Technologies:

SSL Certificate
Issued By:
|- Common Name: Gandi Standard SSL CA 2
|- Organization: Gandi
Issued To:
|- Common Name:

Supported SSL Versions
TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=D0D160DEA05B841B9897507030BCC012; Path=/; Secure; HttpOnly
Strict-Transport-Security: max-age=0
X-Frame-Options: SAMEORIGIN
Cache-control: no-store, no-cache, must-revalidate, post-check=0, check=0
Expires: Thu, 01 Dec 1994 16...
```

Merit Network
Added on 2020-09-06 21:08:09 GMT
United States, Clare

SSL Certificate
Issued By:
|- Common Name: Gandi Standard SSL CA 2
|- Organization: Gandi
Issued To:
|- Common Name:

Supported SSL Versions
TLSv1.1, TLSv1.2

```
HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Content-Length: 0
Date: Sun, 06 Sep 2020 21:08:09 GMT
```

2020-10 - MSBO - Cy | Cyber Security Applie | 20200908 Agenda - G | Extensions - Screen R | American Auto-Matrix | New Tab

shodan.io/host/

Apps | Work | Home | News | Munis | Udemy | Data Breach | Other bookmarks

Shodan | Developers | Monitor | View All... | Show API Key | Try out the new beta website! | Help Center

SHODAN | Explore | Downloads | Reports | Pricing | Enterprise Access | My Account

pool[redacted]-giresd.edzone.net View Raw Data

City	Saint Johns
Country	United States
Organization	Merit Network
ISP	Merit Network
Last Update	2020-09-03T00:06:24.633929
Hostnames	pool[redacted]-giresd.edzone.net
ASN	AS2882

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2018-10549	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\0' character.
CVE-2018-10548	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.
CVE-2018-10545	An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM

Ports

80

Services

80
tcp
http

lighttpd Version: 1.4.18

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
X-Powered-By: PHP/4.4.8
Content-type: text/html
Date: Thu, 03 Sep 2020 00:06:12 GMT
Server: lighttpd/1.4.18
```

2020-10 - MSBO - Cy | Cyber Security Applie | 20200908 Agenda - G | Extensions - Screen R | American Auto-Matrix | New Tab

shodan.io/host/

Apps | Work | Home | News | Munis | Udemy | Data Breach | Other bookmarks

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2018-10549	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\0' character.
CVE-2018-10548	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.
CVE-2018-10545	An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.
CVE-2018-10547	An issue was discovered in ext/phar/phar_object.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-5712.
CVE-2018-10546	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. An infinite loop exists in ext/iconv/iconv.c because the iconv stream filter does not reject invalid multibyte sequences.
CVE-2008-5557	Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.
CVE-2013-4559	lighttpd before 1.4.33 does not check the return value of the (1) setuid, (2) setgid, or (3) setgroups functions, which might cause lighttpd to run as root if it is restarted and allows remote attackers to gain privileges, as demonstrated by multiple calls to the clone function that cause setuid to fail when the user process limit is reached.
CVE-2011-2202	The rfc1867_post_handler function in main/rfc1867.c in PHP before 5.3.7 does not properly restrict filenames in multipart/form-data POST requests, which allows remote attackers to conduct absolute path traversal attacks, and possibly create or overwrite arbitrary files, via a crafted upload request, related to a "file path injection vulnerability."
CVE-2014-5459	The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.
CVE-2009-4143	PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save_path directive.
CVE-2012-2311	sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

```
Server: lighttpd/1.4.18
```

2020-10 - MSBO | Cyber Security Ap | 20200908 Agenda | [redacted] | Extensions - Scree | [redacted] | American Auto-M | American Auto-M | New Tab

Not secure | [redacted]

Apps | Work | Home | News | Munis | Udemy | Data Breach | Other bookmarks

AMERICAN AUTO-MATRIX
A Cylon Energy Inc. Company

Matrix™

ASPECT

Username

Password

Log In

2020-10 - MSBO - Cy | Cyber Security Applie | 20200908 Agenda - G | Extensions - Screen R | American Auto-Matrix | american auto-matrix

google.com/search?safe=strict&sxsrf=ALeKk00IHWbY2xUwpu5eudnRyXdTXTeqhA%3A1599578290275&ei=sqBXX5ayEMXWtQaTjlngBQ&q=american+auto-matrix+aspect+ft+default+username+passwo...

Apps | Work | Home | News | Munis | Udemy | Data Breach | Other bookmarks

Google

american auto-matrix aspect ft default username password

All | Images | Videos | News | More | Settings | Tools | SafeSearch on

About 3,500,000 results (0.51 seconds)

alpscontrols.com › prod_data › new_pdfs › AAMATRIX PDF

Nexus Hardware Installation Guide.book - Alps Controls

and AspectFT-Enterprise are trademarks of **American Auto-Matrix**. ... The AspectFT-Nexus **and** AspectFT-Facility is shipped with a **default IP** address **and** subnet mask. ... When referencing Calendars in **Aspect** Studio, these credentials must be ...

Missing: ft | Must include: ft

www.aamatrix.com › products › aspect-nexus

NEXUS Series - American Auto-Matrix

The NEXUS is an IoT (Internet of Things) embedded **ASPECT**® Control ... Additionally, TCP/**IP** communications using **FT**/Net, BACnet®, Modbus® **and** ... Serial Interfaces, 2 x RS-485@ 9K6, 19K2, 38K4, 57K6, 76K8 or 115K2 (**default** 38K4).

www.aamatrix.com › table › training › Page-2

Training | Table | Page 2 - American Auto-Matrix

The **Aspect** Advanced workshop builds on the knowledge gained from the **Aspect** Basic workshop, **and** project building field experience, ... Engineering Center, Review of setting BACnet **IP** settings within UEC ... **Default** Addressing discussion.

Missing: ft | Must include: ft

aamatrix.com

American Auto-Matrix

Building Automation, HVAC **and** Energy Control leader with over 35 years of industry experience.

Missing: ft | Must include: ft

www.cylon-automatrix.com › products › aspect

ASPECT - American Auto-Matrix

ASPECT is an award-winning scalable building energy management **and** ... Limit **and Default** Improvement; **ASPECT** Alarm Console; Up to 45 exceptions ...

schmid-net.com › american-auto-matrix

ASPECT

Nexus™ & Facility™

Hardware Installation Guide

2.3 Log-In

To log-in to the AspectFT-Nexus and AspectFT-Facility:

1. With your PC's network card configured, open any standard web browser.
2. Browse to the default IP address (192.168.1.251) of your AspectFT-Nexus and AspectFT-Facility.
3. If your connection is successful, you should be greeted with the main page of the Facility, requiring username and password entry.
4. Enter the case-sensitive default username (*aamuser*) and password (*default*) into the fields provided.
5. Click the *Log In* button.

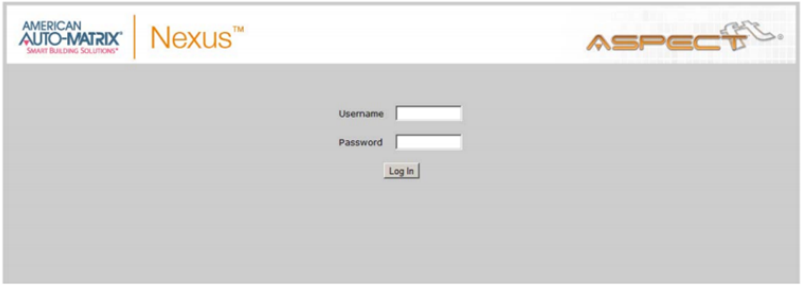


Figure 2-1 AspectFT-Nexus and AspectFT-Facility Log-In

2020-10 - MSBO - Cy | Cyber Security Applie | 20200908 Agenda - G | Extensions - Screen R | American Auto-Matrix | Nexus Hardware Insta

Not secure

Apps | Work | Home | News | Munis | Udemy | Data Breach | Other bookmarks

AMERICAN AUTO-MATRIX
A Cylon Energy Inc. Company

Matrix™

ASPECT

Username aamuser

Password ••••••••

Log In

2020-10 - MSBO - Cy | Cyber Security Applie | 20200908 Agenda - G | Extensions - Screen R | American Auto-Matrix | Nexus Hardware Insta

Not secure | [redacted]/setup.php

Apps | Work | Home | News | Munis | Udemy | Data Breach | Other bookmarks

AMERICAN AUTO-MATRIX A Cylon Energy Inc. Company | Matrix™ | ASPECT

- Aspect Control Panel
  - Application
  - Users and Groups
    - Groups
    - Users
  - Calendar Configuration
    - Calendar File
    - Calendar User
  - Mobile
  - Licensing
  - Communication Setup
    - OOS Manager
    - Port Configuration
    - PUP
    - BACnet
    - Modem Configuration
  - System Administration
    - System Services
    - System Status
    - Process Status
    - License Item Status
    - Project Performance
    - System Updates
    - Backup/Restore
    - Persistence Manager
    - Project Removal
    - Project Source
    - Ethernet Settings
    - Network Diagnostics
    - Time Settings
    - Web Server Configuration
    - Acknowledgements
  - System Logs

User Manager

Add, edit, and delete users.

Add User | Print Users

User	Groups	Delete ☐
aamuser	MIXAdmin -	☐
[redacted]	MIXAdmin -	☐

Delete


Event History
Graphics
Equipment
Floorplans
Ad-Hoc Trends
Saved Trends
Schedules
Network Status
Notification Setup
System Browser
Utilities
256 72.0
257 69.2
221 70.8
220 72.3
231 70.1
233 68.3
214 72.9
234 67.5
213 66.5
122 69.9
66.5
67.0
68.8
204 74.1
66.5
67.0
313 67.2
309
315 67.2
310 73.6
311 74.2
Freezer -3.6 °F
Refrigerator 35.0 °F
76.4
346 71.1
341 71.3
338 71.9
337 76.4
329 69.3
328 69.3
72.0
347 71.7
355 71.3
356 73.1
357 74.5
362 71.9
365 75.3
369 61.3
370 68.7
350 71.5
377 69.6
374 70.7
69.6
456
458 68.0
68.2
430 68.0
429 70.8
72.1
69.7
68.8
71.1
404b 67.2
404a 70.2
407 74.1
68.8
71.0
72.0
72.7
71.6
71.7
Legend
Corridors
Uncontrolled Area's
100 Wing
200 Wing
300 Wing
400 Wing

Not secure | [redacted]cgi-bin/sri_config.cgi?pr

Apps ★ Work Home News Agendas

Please click Update button after making a change

Board IP Settings

Hostname: SRI-06-14927

- ○ DHCP
- ◉ Static

IP Settings

IP Address: [redacted]

Subnet mask: 255.255.0.0

Default gateway: 10.23.0.254

- ○ Obtain DNS Server Address Automatically
- ◉ Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS: 10.2.0.222

Secondary DNS: 8.8.8.8

☑ Enable Ether Link Auto Negotiation

CIM IP Address Setting

IP Address or Hostname: [redacted]

Port Number: 3001

VSRC Lock (Relay 1) Configuration

Comm. Failure

- during MRO
- ○ Retain State
- ○ Unlocked
- ◉ Locked

Power On

- ○ Unlocked
- ◉ Locked

Update Display

VSRC Lock (Relay 1) Configuration

Comm. Failure

- during MRO
- ○ Retain State
- ○ Unlocked
- ◉ Locked

Power On

- ○ Unlocked
- ◉ Locked

Update Display

Basic CIS Controls

1. Inventory and Control of **Hardware** Assets
2. Inventory and Control of **Software** Assets
3. Continuous **Vulnerability** Management
4. Controlled Use of **Administrative** Privileges
5. Secure **Configuration** for Hardware and Software
6. Maintenance, Monitoring and Analysis of **Audit Logs**

Control 1: Hardware Control

- What servers, workstations and devices do you have that control Facilities and are critical to daily operations?
- Are these physically secured? Who can get at them?
- Who is regularly maintaining them? How often?

Steps to Take:

- Keep accurate **asset lists** and **point of contact**
- Ensure **physical security**
- **Regularly** review and update this list

Control 2: Software Control

- Can you easily identify and report on the software versions running on your Facilities Systems?
- When was the last time you updated the Operating System or software version?

Steps to Take:

- Keep accurate **software lists**
- **Remove the ability** for local software installs
- Know **who** is responsible for maintaining each system

Control 3: Vulnerability Management

- Are your systems operating systems and software up-to-date?
- Is antivirus or malware detection enabled on the system?
- Are there systems you simply cannot update?

Steps to Take:

- Ensure vendors or your IT department are keeping your systems patched and updated.
- Set up a schedule to scan your systems or at least check for updates.
- Isolate old/vulnerable systems from the network

Control 4: Admin Accounts

- Is the password for your account the default?
- Is your Admin account secure? Longer is better!
- Can you access the interface via a web search or sticky note?

- **Steps to Take:**
  - Keep **audited** inventory of admin accounts
  - **Change default passwords**
  - **Use dedicated computers and accounts** for administrative tasks in conjunction with **two-factor authentication** where possible.

Control 5: Secure Configurations

- Did anyone review the system before deployment?
- How are you/vendors accessing the site remotely?

Steps to Take:

- Regularly **review** list of vendors with external access
- Enable VPN users access **only when needed to complete work** (Work with your IT staff to maintain a secure perimeter.)

Control 6: Audit Logs

- Can you **fully** recreate events to aid in troubleshooting and incident response?

- **Steps to Take:**
  - Enable **detailed logging** in software as well as on all servers and workstations
  - Create **alerts** to notify Facilities and IT staff on suspicious activity.
  - **Ask questions** about log entries

Suggestions

Schedule regular checkups & audits
Talk to your techs regularly
How can we do this securely?
Review logs regularly & investigate

Suggestion for Bids / Working with Vendors to Secure Systems on Day 1

- Add language to RFP/RFB regarding security
  - Two factor authentication, secure remote access
  - Software updates/maintaining a secure configuration
- No open /backdoor access from the Internet
- Anti-virus compatibility
- Consider inviting IT dept to review for information security concerns

Suggestion for Bids / Working with Vendors to Secure Systems on Day 1

Ensure your business office has the correct vendor information!!!

A district in Michigan fell victim to a wire transfer fraud. Hackers exploited district by posing as the winning bidder and requesting payment. A six figure sum was wired to the hackers bank account.

Credits & contacts

Matt McMahon mmcmahon@giresd.net
Joel Phillips jphillips@ncresa.org
Merri Lynn Colligan mcolligan@washtenawisd.org
David Larson davidlarson@livingstonesa.org

MiSecure http://www.misecure.org/
2021 Data Breach Investigation https://enterprise.verizon.com/resources/reports/dbir/