AMERICAN BANKRUPTCY INSTITUTE

2019 Hon. Eugene R. Wedoff Seventh Circuit Consumer Bankruptcy Conference

Technology-Related Ethical Issues

Hon. Beth E. Hanan
U.S. Bankruptcy Court (E.D. Wis.); Milwaukee

David P. Leibowitz
Lakelaw; Waukegan, Ill.

Thomas P. O'Hern
ICF International, Inc.; Fairfax, Va.

CONCURRENT SESSION

2019

Legal Ethics and Technology

"Crisis = Challenge + Opportunity"

Panelists

Hon. Beth E. Hanan *U.S. Bankruptcy Court (E.D. Wis.); Milwaukee*
David P. Leibowitz *Lakelaw; Waukegan, Ill.*
Thomas P. O'Hern *ICF International, Inc.; Fairfax, Va.*

Legal Ethics

ABA Model

Model Rules of Professional Conduct, Rule 1.1: Competence - A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment under "Maintaining Competence" - [8]: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Cite: MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N)

WI

Wisconsin Rules of Professional Conduct, Supreme Court Rule 20:1.1 (2007, last amended in 2019):Competence - A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

ABA COMMENT [8]: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Cite: WI RULES OF PROF'L CONDUCT r. 20:1.1 cmt. 8

IL

Illinois Rules of Professional Conduct, Rule 1.1 (2010, amended to reflect technology in 2016): Competence - A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment [8]: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in

continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject

Cite: IL RULES OF PROF'L CONDUCT r. 1.1 cmt. 8

IN

Indiana Rules of Professional Conduct, Rule 1.1 (1987, last amended 2019): Competence - A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment [6]: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with the technology relevant to the lawyer's practice, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Cite: IN RULES OF PROF'L CONDUCT r. 1.1 cmt. 6

MO

Missouri Rules of Professional Conduct, Supreme Court Rule 4-1.1 (1985, last amended 2017): Competence - A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment [6]: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject.

Cite: MO RULES OF PROF'L CONDUCT r. 4-1.1 cmt. 6

Note

Michigan does not appear to have adopted the Comment, yet.

Technical Outline

1. Your Biggest Threats
    a. The computer user – easiest target and conduit to protected networks, systems & data
    b. Ransomware Malware Infection – permanent data loss scenario
    c. Theft of mobile computer or storage media
    d. Insecure Remote Access – to privileged and user accounts especially Internet access
    e. PII - Data at Rest, Data In Transit, Data in Use
2. The Basics: Information Technology (IT) Cyber Security Principles
    a. Information security is built on Confidentiality, Integrity and Availability (CIA) of data
    b. Security posture is a product of your technical, operational and physical security
    c. Everyone's is situation is unique.
    d. Risk Management Lifecycle

i. Assess what you have, determine what needs to be protected, determine how to protect it, implement the protections, verify the protections, and repeat.
ii. Provide a cost effective prioritization of high risk items for remediation.
iii. Lifecycle process address persistent change and allows maturing of security posture over time.

3. Where to Start
    a. Inventory and Asset management (Hardware, Software, Data)
        i. * A Master Password List
        ii. * Two Birds with One Stone - NACTT Quarterly Article
    b. Risk Assessment
        i. Physical Security – Access control to equipment, storage media , & documents)
        ii. Operational Security – Policy, Plans and Procedures in practice
        iii. Technical Security – to follow …
4. Technical Security - Building Layers of Defense – The Basics
    a. General Security Notes
        i. Buy mainstream US or allied nation security products and equipment
            1. Not Huawei, Kaspersky, Lenovo
    b. Timely system administration and maintenance is the foundation of security
        i. Patches and Updates
            1. NOTE: Jan 2020 - Microsoft stops support for 2008 Svr and Win 7, budget and plan to update now.
            2. Use Microsoft Auto-update on PCs
            3. Patch servers monthly
            4. Patch 3rd party software applications monthly, use auto update features
            5. Network device firmware updates – firewalls, routers, switches, wireless
        ii. * Administration Checklist tab in the Master Password spreadsheet
    c. Secure your Data
        i. Data Management Plan*
            1. Data In: Receive, Reject, Redact,
            2. Data You Have: Backup, Archive
            3. Data Not In Use: Reduce, Remove, Destroy
            4. Data You Transmit: Encrypt, Encrypt, Encrypt
        ii. Data In Transit – Client/Server Network communications
            1. Use of SSL/TLS for common network service
                a. Email: POP, IMAP vs POP/S, IMAP/S
                b. Web: http vs. https
            2. Encrypt data first when transmission is unencrypted
        iii. Data At Rest – Stored Data
            1. Full Disk encryption of computer hard drives
            2. Encrypted backups (Who has the key and key password?)
            3. Secure file sharing and exchange*
        iv. Data In Use – a Users perspective
            1. Line of sight & Screen locks
            2. Keep the data in the office (ex: Remote Desktop over VPN)

3. Strong User authentication + Access Control Permissions to secured data
4. Programmatically mask data fields

d. Secure Your Access
   i. NOTE: Username and password are insufficient to login over the Internet.
   ii. Use 2-factor, multifactor, 2-step authentication for all logins over the Internet
      1. Use for VPN logins accounts for remote access into the office network.
      2. Enable on Websites and Cloud Services
      3. and require on all cloud service accounts
      4. …
e. Securing Your Devices
   i. Desktop Computers security suite software with subscription
      1. McAfee, Symantec, Microsoft Defender
      2. Anti-virus, malware, spam filtering, application firewall,
   ii. Mobile devices, laptops, tablets and smart phones
      1. Bootup passwords and Disk encryption (Windows BitLocker)
      2. Remote Wipe,
   iii. Servers
      1. Enable encryption on the hard drives or filesystems
      2.
f. Secure your Network
   i. Next Generation (NG) Firewall (All in one)
      1. Sonicwall, Fortinet, WatchGuard, PaloAlto
      2. Deny all, Allow by exception
      3. Intrusion detection/prevention (subscription based updates)
      4. Web filtering (inbound and outbound)
         a. Geo-IP filtering by country
         b. Categorical web filtering
   ii. Virtual Private Network (VPNs)
      1. Provide
         a. Trustworthy user authentication for access control
         b. Encrypted communication between members
      2. Use for all remote access into secure network
      3. Use when communicating over any wireless network
   iii. Wireless Networks
      1. Are inherently insecure
      2. Keep them separate from your trusted network
      3. Connect them to the firewall and require VPN connection to access secured office network
      4. Or allow Internet access
g. Secure your Critical Services
   i. Email
      1. NOTE: Forbid use/access to personal webmail services. Backdoor for infections.

2. Pre-delivery SPAM filtering
    a. before it gets to the user's mailbox and for all outbound email
    b. Included with Microsoft O365 for $1/user/mth, Appriver
3. SPAM filtering plugins for email clients
4. www.mxtoolbox.com Check your email domain security features
    a. TKIM, DMARC, DNS, Blacklists and more

ii. Websites – Content, Application, Web service, Server
1. Annually review content
2. Review and approve updates
3. Patch and maintain the Web App, service and server
4. www.ssllabs.com Tool to check security setup of website

iii. Cloud Services

h. Secure your Operations
i. Disaster Recovery (DR) or Continuity of Operations (CoOP)
1. DR: planning for failure - Backup and Restoration
2. CoOP: Continue to operate from anywhere
    a. Separating people, computing and data from the office
    b. Paper - Going paperless – electronic records
    c. Data backups - Online backup and cloud storage
    d. Servers - Virtual servers to cloud servers
    e. Email - Hosted Exchange and Office 365
    f. Software applications - applications in your browser
    g. Phones - Internet Phones - Voice Over IP (VOIP)
    h. Fax - Cloud fax services
    i. Desktop computer - Laptops, Virtual Desktop in browser, BYOD

ii. Computer Use Policy – Outlines the Dos and Don'ts
iii. Train your Users (Focal Point)
1. Annually on basic practices and computer user policy
2. *Basic Malware Protection Practices: SAVE-SCAN, INSPECT
3. *Basic Incident Response: STOP-DROP-CALL
4. Perform annual computer security awareness training
    a. www.knowbe4.com

iv. * Incident Response Plan
v. * Cyber-Liability – When all else fails, the last layer of defense.
1. For 2018 IBM Reports $154/record
2. x 2 for Debtor and Spouse
3. x # cases online

i. Miscellaneous Topics and Questions? (time permitting)

Supplemental Material

*- Technical Referenced Materials

1. Master Password List spreadsheet & NACTT Quarterly Article – Two Birds – One Stone (PDF)
2. Malware Protection Poster
3. Applicable NACTT Quarterly Articles Available Online
    a. Email: Our Daily Threat
    http://www.ezflipmags.com/Publications/NACTT_Quarterly/18/#p=5
    b. Email Encryption
    http://www.ezflipmags.com/Publications/NACTT_Quarterly/24/#p=5
    c. OMG, They Are All Administrators
    http://www.ezflipmags.com/Publications/NACTT_Quarterly/25/#p=5
    d. Cyber Liability Insurance (CLI) – Candy Gross of International Sureties
    http://www.ezflipmags.com/Publications/NACTT_Quarterly/26/#p=7
    e. Incident Response and Data Breach Notification
    http://www.ezflipmags.com/Publications/NACTT_Quarterly/28/#p=6
    f. Computer Incident Response
    http://www.ezflipmags.com/Publications/NACTT_Quarterly/29/#p=7
    g. Let's Go Phishing
    http://www.ezflipmags.com/Publications/NACTT_Quarterly/30/#p=6
    h. Spring Cleaning: Do You Have a Data Management Plan
    https://www.ezflipmags.com/Publications/NACTT_Quarterly/31/#p=6
    i. IT Support Vendors: A Case study of Risk, Dependencies, & Accountability
    https://www.ezflipmags.com/Publications/NACTT_Quarterly/34/#p=8
    j. Web Applications Security Risks
    https://www.ezflipmags.com/Publications/NACTT_Quarterly/36/#p=6

Other References

    k. NIST Documents
        i. NISTIR 7621Rev1: Small business Information Security: The Fundamentals 53 – Page good read for IT novice business person with practical guidance
        https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
    l. Small Medium Sized Business Firewalls
        i. https://www.esecurityplanet.com/products/top-ngfw-vendors.html#NGFWcomparison

Fundamental Professional Responsibility

From the preamble:

4] In all professional functions a lawyer should be competent, prompt and diligent. A lawyer should maintain communication with a client concerning the representation. A lawyer should keep in confidence information relating to representation of a client except so far as disclosure is required or permitted by the Rules of Professional Conduct or other law.

From the definitions:

[9] The purpose of screening is to assure the affected parties that confidential information known by the personally disqualified lawyer remains protected. The personally disqualified lawyer should acknowledge the obligation not to communicate with any of the other lawyers in the firm with respect to the matter. Similarly, other lawyers in the firm who are working on the matter should be informed that the screening is in place and that they may not communicate with the personally disqualified lawyer with respect to the matter. Additional screening measures that are appropriate for the particular matter will depend on the circumstances. To implement, reinforce and remind all affected lawyers of the presence of the screening, it may be appropriate for the firm to undertake such procedures as a written undertaking by the screened lawyer to avoid any communication with other firm personnel and any contact with any firm files or other ~~materials~~ information, including information in electronic form, relating to the matter, written notice and instructions to all other firm personnel forbidding any communication with the screened lawyer relating to the matter, denial of access by the screened lawyer to firm files or other ~~materials~~ information, including information in electronic form, relating to the matter, and periodic reminders of the screen to the screened lawyer and all other firm personnel.

From the rules:

RULE 1.1: COMPETENCE

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

…. Comment 8:

Maintaining Competence

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject

RULE 1.6: CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b) or required by paragraph (c).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent the client from committing a crime in circumstances other than those specified in paragraph (c);

(2) to prevent the client from committing fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; ~~or~~

(6) to comply with other law or a court order; or~~.~~

(7) to detect and resolve conflicts of interest if the revealed information would not prejudice the client.

(c) A lawyer shall reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary to prevent reasonably certain death or substantial bodily harm.

(d) Information received by a lawyer participating in a meeting or proceeding with a trained intervener or panel of trained interveners of an approved lawyers' assistance program, or in an intermediary program approved by a circuit court in which nondisciplinary complaints against judges or lawyers can be referred, shall be considered information relating to the representation of a client for purposes of these Rules.

(e) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

RULE 3.4: FAIRNESS TO OPPOSING PARTY AND COUNSEL

A lawyer shall not:

(a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act;

(b) falsify evidence, counsel or assist a witness to testify falsely, or offer an inducement to a witness that is prohibited by law;

(c) knowingly disobey an obligation under the rules of a tribunal, except for an open refusal based on an assertion that no valid obligation exists;

(d) in pretrial procedure, make a frivolous discovery request or fail to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party;

(e) in trial, allude to any matter that the lawyer does not reasonably believe is relevant or that will not be supported by admissible evidence, assert personal knowledge of facts in issue except when testifying as a witness, or state a personal opinion as to the justness of a cause, the credibility of a witness, the culpability of a civil litigant or the guilt or innocence of an accused; or

(f) request a person other than a client to refrain from voluntarily giving relevant information to another party unless:

(1) the person is a relative or an employee or other agent of a client; and

(2) the lawyer reasonably believes that the person's interests will not be adversely affected by refraining from giving such information.

Adopted July 1, 2009, effective January 1, 2010.

Comment 2:

[2] Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party, including the government, to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for purpose of impairing its availability in a pending proceeding or one whose commencement can be foreseen. Falsifying evidence is also generally a criminal offense. Paragraph (a) applies to evidentiary material generally, including computerized information. Applicable law may permit a lawyer to take temporary possession of physical evidence of client crimes for the purpose of conducting a limited examination that will not alter or destroy material characteristics of the evidence. In such a case, applicable law may require the lawyer to turn the evidence over to the police or other prosecuting authority, depending on the circumstances.

Lessons Learned

Over the last year, the STACS team has observed an increased turnover of system managers supporting Standing Trustee offices. Our initial response to this issue was to compile information from across the community and develop guidance for Trustees on hiring a system manager. The guidance is available for download from the STACS website library and contains a sample job description, candidate search information, interview questions and a template to track and compare candidates.

We recently had the opportunity to provide onsite support to an office that experienced an unexpected departure of their system manager. The STACS team provides emergency onsite support services as feature of the STACS program to assist offices in assuring full, secure and adequate control over critical computer systems, networks and operations. As part of this process, we perform an after action evaluation to identify items that could help prevent or minimize the impact of these types of events. We frequently discover valuable and practical information worth sharing with the community at large as lessons learned. In this particular case, we focus on lessons learned involving the maintenance of password lists and basic system documentation.

Background

While onsite, we were provided a lengthy list of administrative usernames and passwords for the variety of network devices, computer systems and software applications. Working through the password list, we realized some key passwords were missing, some were not up-to-date, others belonged to legacy systems no longer in use and in some cases, we just could not find the right software on the right system. With little to no documentation available, hours were spent trying to locate critical applications and backups of system, software and device configuration files.

In the cases where key passwords were missing, complete systems had to be rebuilt, reinstalled and reconfigured. Obtaining vendor support for products with active maintenance agreements became difficult when we discovered the products were only registered under the former system manager's name. Adding fuel to this fire was our discovery that the vendor no longer distributed the required software to reinstall the device. Without the password and software, the device was rendered useless and needed to be replaced.

The rebuilt systems were configured with our best guess attempt to restore the original configuration. However, some critical functionality was lost until problems were discovered and eventually resolved days or weeks later.

Many hours were also spent locating components of undocumented systems and investigating their configuration settings to determine enabled system features and functionality.

Systems that had updated passwords and documentation allowed for rapid password changes and configuration updates to assure the system's security.

Two Birds, One Stone

Many offices are challenged with compiling and maintaining accurate administrative password lists as well as developing basic system management documentation. You can kill two birds with one stone by implementing a periodic (quarterly) audit of the administrative password list. The audit allows you to maintain the currency of the passwords and verify the existence and accuracy of basic documentation needed to use each account credential on the list.

Let's examine a practical approach to create a comprehensive list and easily develop basic procedural documentation for each account.

The List

Tracking the Elements. For each account and password in your list, include the following data elements:

- Date – of last verified password update change

- Account Credentials – the usernames, passwords or passphrases
- Location – describes how to get to the location where the credentials can be used. Include any special requirements or access restrictions such as you must log in from a specific computer or user account. Examples:
    - Hostname (ex: AVServer)
    - Network Address (ex: 192.168.1.5)
    - Website (ex: from the IT managers computer go to https://avserver:9000/)
    - Hostname/Account/ProgramName (ex: AVServer, domain\Administrator, AV Console Manager)
- Description – provides the purpose, usage or common tasks performed with this account. (ex: centralized antivirus management to configure and update AV software on all computers)
- Documentation – indicates location of associated documentation or references to a specific procedure
- Configuration Backups – if not included in the system documentation, indicate where the configuration files are backed up.

Building the List. It is critical to identify all of the account credentials (username and password) required to manage and operate the systems that support your office. It is not always easy to enumerate all of these critical accounts, but the categories we described below should help with this process.

It's important to note, there may be multiple accounts and passwords needed to manage a system or device. For instance you may be required to log into (1) a specific account such as the domain administrator account on a specific computer, (2) open an application or browser and log into a system management program, (3) use a password to read and edit the current configuration, and (4) use another password to permanently save new configuration changes.

Computer Systems, Servers and Network Devices are the easiest accounts to identify. Most have a local administrator account to manage the device and also use domain administrator account if they belong to a managed network of computers.

Network Devices like routers and firewalls often require multiple passwords to perform critical administrative tasks. Long passwords called passphrases are used by network devices to control network access such as in the case of a wireless network. Passphrases are also used to establish encrypted network connections called Virtual Private Networks (VPN) to remote users and remote networks. Other networked devices frequently overlooked include switches, printers, and All-in-One print-scan-fax-copy machines.

Specialty Systems provide critical business functions and are often installed by outside vendors. They tend to sit untouched in the office for year and are often the systems with the worst security. These systems support phone and voice mail, postage, teleconferencing, time cards, alarm and badging, video and closed circuit TV.

Any of the systems or devices above can require the installation of management software on separate computer from which they will be remotely administered. If the ***Management Software*** requires a username and password be sure to include this on your list.

Business Applications also use internal administrative accounts to limit access to software configuration settings and program features. Products like antivirus, patch management, case management, databases, and webservers all have important usernames and passwords to track.

External Service Providers offer a wide range of services and products to Trustees. Many providers issue web portal accounts to their customers to purchase and register products, issue and distribute licenses, provide and track maintenance and support assistance.

"It's vital that service accounts are created and issued with the name, email and physical address of the Trusteeship to avoid confusion over ownership and use of vendor services."

Service provider accounts to include on the list: the Internet Service Providers (ISP) that issue your public Internet addresses and provide your Internet access, the domain name registration service that translates your hostnames like www.mych13.com to an Internet IP address, any outsourced hosting service such as email or SPAM filtering, online backups or website services. Include master accounts used to create and manage individual accounts for staff. Examples might include master accounts for a case vendor websites, ECF or PACER.

Finally, and most importantly, include are E***ncryption Passwords and Passphrases***. Without them, the data they protect is unrecoverable. These passwords are commonly used to encrypted backups, portable hard drives, and USB thumb drives.

Protecting the List.

Although there are software programs available on the market to store and track usernames and passwords, a password protected Excel spreadsheet that is stored on a password protected and encrypted USB thumb drive can be a simple and effective solution. Setting the Open password on the spreadsheet provides protection when the USB drive is mounted on a computer system. The password and encryption of the USB thumb drive provides protection in case the thumb drive is lost or stolen. A good addition to the thumb drive would be the latest version of the documentation we describe below.

The Documentation

The lack of good system level documentation is a common issue across the community. Whether it is disdain for the task, under appreciation of its usefulness, or administrator's strategy for self-preservation, systems managers generally don't like doing documentation. However, if it's important enough to require a password, it's important enough to document.

One method I find to be extremely useful for developing system level documentation is to document in pictures. Most desktop operating systems provide a Print Screen (Ctrl-Alt-Prt Sc) feature to capture an image of the desktop or selected application window. The image is stored in the system clip board and can be pasted directly into a Word document. An administrator can quickly create a visual representation of an administrative procedure then provide a short description of each image if necessary.

Screen captures are also good for documenting configuration setting that are otherwise hard to replicate or reproduce for documentation. For instance, we frequently take screen captures of firewall rules during our onsite assessments to help use recall or review these settings.

Summary

Your master password list is a living and breathing document that needs to be vigilantly maintained for the unanticipated situations when your IT support person is unavailable. Implementing an internal quarterly audit of the list assures critical passwords are being changed regularly, they are being kept up to date and procedures for each account are developed and maintained with current information. Coupling a master password list with some basic system documentation will minimize the stress and struggles of losing a system manager, accelerate the transition process to a new system manager and help with disaster recovery and response efforts.

One final note, although this article focused on system managers and system administration, the same approach can be applied by comptrollers and office managers to create a master list and basic documentation for Trustee financial and operational accounts and services.

Need Help?

The STACS team can be contacted to provide further technical guidance and assistance at ***support@stacs.net*** or by calling ***866-STACSNEt***.⊙

- *Authored by Thomas P. O'Hern*
- 

ALERT MALWARE ATTACKS ALERT

As a computer user, **YOU** are targeted by hackers to help provide unauthorized access to your computer and it's data. Hackers use malware (malicious software) to remotely access your computer and steal data. Hackers use authentic looking email messages with file attachments or misleading website links to distribute their malware. Website links can direct your browser to download and install malware or direct you to hacked websites where passwords or other sensitive information is solicited.

COMMON SIGNS OF MALWARE

- Email attachments with unusual file name extensions: .exe, .zip, .scn, .ZIP, .PDF.exe
- Email attachments that do nothing when opened or prompt for installation approval
- Website links in email to IP addresses, foreign countries, or unusual hostnames

PREVENTION

If you must open an email attachment or file downloaded from the Internet,

SAVE the file without opening or executing it, then

SCAN the files with anti-virus software that is updated daily with new virus detection signatures.

INSPECT suspicious website links in email and web pages. Hovering your mouse cursor over a link should display the real location in a pop-up window or web browser status bar.

RESPONSE

If you think you accessed, opened or executed malware:

STOP immediate response is critical in containing the damage.

DROP your computer's network connection by turning off the wireless network or unplugging the network cable from the wall or computer.

CALL your system manager, office manager or STACS to help triage the situation and plan effective response and recovery actions.

STACS SUPPORT | 866-782-2763 | support@stacs.net

MALWARE ATTACKS

PREVENT: Save, Scan, Inspect

RESPOND: Stop, Drop, Call

STACS Support 866-782-2763

Last Update	Account Name	Password Passphrase	Location	Description	Documentation Reference	Backup Config Files
Special Data Encryption Passwords/Passphrases						
				Master Password Database - password and database file		
				Encrypted Backups PassPhrase		
				Quickbooks encrypted USB memory stick backup		
	Trustee			Quickbooks Account		
Servers and Desktop						
	ch13\administrator		Domain Server	Domain Administrator account		
			Database server	Database Administrator account		
			Desktops	local administrator account on all desktops, laptops, servers		
				Virtual Server - HyperVisor credentials		
				BIOS boot and Disk Encryption password(s)/passphrases		
Network Devices and Remote Network Access Services						
	administrator		https://192.168.2.1/	Internet Router		
				LAN Switches		
	user1		https://192.168.0.1/	Office Firewall Appliance - Read Only		
	Admin		https://192.168.0.1/	Office Firewall Appliance - Read/Write		
	Administrator		IT mananger PC; Login as domain administrator; run ManageMyFW application	Office Firewall Management Server Service Account		
				Office Firewall Site-to-Site VPN Passphrase		
	admin		341 room utility closet connect to physical port 1 browse to https://192.168.3.1/	341 room WiFi Router	SM Manual - Procedure 3	
	CH13-341		341 room connect to CH13-341 wireless network	341 room Public WiFi SSID & Passphrase		
	ABCVendor admin			ABC Vendor PCAnywhere account VPN administrative account		
				PVN Shared Passphrase		
Specialty Systems						
				Phone System		
				Phone System Management Software Server account		
				Voice Mail Server		
				Teleconferencing System		
				Security Camera System		
				Alarm System		
				Badging System		
				Time Clock System		
				Postage System		
				Scanner		
				Fax		
				Printer(s)		
				Check Printer		
Business Application Software Services						
				Centralized Antivrus management service		
				SPAM filtering service account		
				Corporate Website management account		
				Email server administration account		
				Public Website administration account		
				Case management administration account		
				Database Administration account		
External Service Provider Accounts						
				Antivirus Software Vendor Maintenance account		
				ABC Computer System maintenance service account		
				Internet Service Provider customer account management		
				Internent Domain Service customer account management		
Cloud or Hosted Service Provider Administrative Account Credentials						
				Email		
				SPAM filtering		
				Multifactor authentication		
				Online banking		
				Epay		
				TFS		

Novice Admin

Antivirus & Spyware	**Immediate**	**Daily**	**Weekly**	**Monthly**	**Quarterly**	**Yearly**
AV signature updates		X				
AV software updates		X				
Real-time scan of new files on servers and desktops	X					
scan of servers and desktops hard drives			X			
Confirm central AV management of all servers and desktops				X		
License renewals						X

Check & confirm monthly

Backups	**Immediate**	**Daily**	**Weekly**	**Monthly**	**Quarterly**	**Yearly**
Server and application configuration and configuration changes	X			X		
Critical application data, databases and file servers		Inc/Full		Full		
Email		Inc		Full		
Device Configurations: Firewall, VPN, Router	X			X		
Tape media replacement				X	X	X
Backup restoration test				X	X	

Restore file from backup monthly

Patch Management	**Immediate**	**Daily**	**Weekly**	**Monthly**	**Quarterly**	**Yearly**
Desktop operating systems and application updates		X				
Server operating system and application updates			X	X		
Third party application updates			X	X		

Patch all systems monthly

Log Reviews	**Immediate**	**Daily**	**Weekly**	**Monthly**	**Quarterly**	**Yearly**
Critical data backups logs for success or error		X				
AV & Spyware scan logs for infections & successful updates			X			
Remote access account logs for failed logins and unusual login times/locations			X			
Server and desktop security logs for failed logins and unusual login times			X			
Server and desktop application and system event logs for critical errors				X		
Firewall, VPN, IDS, SPAM alert logs for critical events	X	X	X			

Account Management	**Immediate**	**Daily**	**Weekly**	**Monthly**	**Quarterly**	**Yearly**
Disable dismissed employee accounts & shared account password changes	X					
Review remote access accounts			X			
Review, disable, backup and remove old users accounts				X	X	X
Reset temporary privelages on user accounts	X		X	X		
User account password changes					X	
Shared account password changes						
Review user permissions and group membership settings				X	X	

Review quarterly

Miscellaneous	**Immediate**	**Daily**	**Weekly**	**Monthly**	**Quarterly**	**Yearly**
Verify access permissions on file servers and network share folders					X	
Check SPAM filtered files for real messages		X	X			
Renew critical software licenses: business applicaitions, AV, software maint.						X
Renew critical support and service contracts: HW maint., ISP, email, webhosting						X
Budget for upgrades or new hardware, software, network equipment						X

Weekly

Task ID	Task Description	Priority	Status	Completed By	Date
	Verify Recent Data & System Backups				
	Case Management Database	High			
	Employee PC - Full system backup	High			
	Exchange Server - Full sysetm backup	Med			
	Employee's Email box - monitor email to account: share mailbox	High			
	Employee's home directory on the fileserver	High			
	Retension of all data tape backups from Case Server and Exchange Server	High			
	Accounting Software database	High			
	Change Account Passwords				
	Case Vendor - Remote access accounts (Pcanywhere, SSH, gotomypc, logmein, etc.)	High			
	Case Vendor - Trustee accounts to access case vendor websites	High			
	Case Vendor - VPN account	**High**			
	Case Vendor - FTP account for data transfers to vendor	High			
	Case Vendor - Internal administrative database accounts (sa, ora_admin, etc.)	High			
	Case Vendor/Office - Validate list of internal database user accounts, (lockout unknown accts)	**High**			
	Case Vendor - website accounts for Trustee staff and automated tasks	High			
	NDC - Accounts	High			
	STACS - All accounts passwords reset	High			
	ECF - (http://pacer.psc.uscourts.gov/) All accounts	High			
	ECF FTP site account - oconnell account (ftp://www.txs.uscourts.gov/)	High			
	Office website account password	High			
	Trustee - All Domain User Accounts	High			
	Trustee - Local administrator accounts on all office computer systems	High			
	Trustee - All VPN accounts	High			
	Trustee - Firewall Admin Account	High			
	Trustee - Phone Call Accounting system	High			
	Trustee - Virus Management system	Med			
	Trustee - Email accounts and management accounts				
	Internet Service Provider (ISP) - Router Admin Account (if known)	Med			
	ISP - Web Portal account	Med			
	Internet Domain Name Registrant Account - Web portal account				
	Trustee - Voice Mail passwords for each extention	High			
	Trustee - Voice Mail/Phone system administration account	High			
	Voice SP - Verify need to modem connectivity to Voice Mail system	High			
	Payroll - Online payroll account for Employeer and Employee	High			
	Payroll - Online payroll account for other payroll managers	High			
	Bank - Electronic account access	High			
	Bank - Signature cards for safety deposit box	High			
	AMEX - Corporate Card online account management	High			
	AMEX - Subject's card closure	High			
	Office HR - 401K retirement account management	High			
	Office HR - Medical Insurance services accounts	High			
	Online Services and Support Accounts (closure and password changes)				
	Change router/firewall administrative account passwords	High			
	Expire and require password changes on all office network/computer accounts for all empoloyees	High			
	Corparate Credit Card Accounts	High			
	Application Service Providers (email, web site, etc)	Med			
	Internet Service Provider	Med			
	Corporate postage account	Med			
	Cellular phone service account	Med			
	Fedral Express service account	Med			
	Efiling service account for quarterly tax payment	Med			
	Electronic Bankruptcy Noticing (http://www.ebnuscourts.com/)	Med			
	TENs account (http://www.trusteenet.org/)	Low			
	NACTT account (www.nactt.org)	Low			
	Company Travel Manager Accounts	Low			
	Add any additional online accounts for purchasing office supplies/equipment/software/software licneses	High			
	Consider implementing an email list like systems@trustee.com for online service account login and email contacts	med			
	Physical Security				
	Change PIN/Passcodes on Alarm systems	High			
	Obtain and review security system access records	High			
	Inventory any company credit cards stored in the office	High			
	Inventory any keys stored in the office	High			
	Inventory onsite backup tapes to ensure that they are all accounted for	High			
	Replace locks on all external doors	High			
	Install an office burglar alarm	High			
	NOTE: The removal of paper documents may not be evident immediately				

Outline of general To Dos to prioritize for Key Employee Dismissal:

At time of dismissal
- Issue mailbox deletion for sync'd mobile device(s) listed under the user's account on the Exchange server
- Change domain password of user account when mailbox sync removal is confirmed
- Inquire about remote access products VPN/3rd party programs and services and credentials to access hosted ren
- Disable users VPN account and change firewall admin password(s)
- Review outstanding VPN account and change other account passwords if known to user
- Change WiFi and router admin passwords and check for other local accounts
- Change Domain administrator account and verify other domain admin accounts
  - Check antivirus and backup agent cached credentials and update if running under the domain/Administrator acc
- Start scan of network computers and review installed software for remote access programs
- Physical security and camera system accounts
- Perform a review of user's laptop/computer for Trustee email, documents and other references to Trustee related
  - Review file system
  - Browser (history, stored password lists and book marks).
  - Installed or frequently used programs for indications of Trustee related use
- Review scan results for and high risk vulnerability and unauthorized or remote access software

In parallel with the above activity, someone can contact the non-technical services or parties to change passwords,
- Review Master password list for credentials to prioritize password changes and update contact information if nece
  - Start with any financial account access (SunTrust, Dropbox,)
  - Other Bankruptcy related accounts (BSS, Courts, 13 docs, NDC, STACS, …)
  - Network related accounts (DNS, Telephone, IPS, Domain Registrar, Email/SPAM filtering)
- Contact Case Software Vendor
  - Change 13software.com master password. Note: All user passwords are visible to admin users.
  - Review other user accounts and change as needed.