INSIDER THREAT DEFENSE GROUP

Security Behind The Firewall Is Our Business

Teleworking Guidance To Mitigate Employee Risks

This document was written by the Insider Threat Defense Group to provide guidance on mitigating employee risks while teleworking.

Unfortunately the impact of the Coronavirus is being felt here in the U.S. and globally. Marriott International, the world's largest hotel company, said tens of thousands of hotel workers will be furloughed, and will layoff a number of those workers. There are many other companies in the U.S. that are reducing their workforce through furloughs and layoffs. According to a Washington Post article, workers are struggling to apply for unemployment aid as government websites crash and phone lines have hours-long waits. Then some are finding they don't even qualify for help.

In many states employees' working for nonessential businesses are required to stay home in an effort to combat the spread of the Coronavirus. Other businesses are having employees' work from home via teleworking.

Businesses should understand that many employees' are going through various levels of concern and anxiety over this virus outbreak. This is adding to the daily stress of working and being productive. Before the virus outbreak some employees' may have already been experiencing financial problems, or other work related or external stressors. Some employees' are having their income reduced. All this stress and reduced income, could possibly lead to an employee into justifying taking some form of action against their employer that might cause harm. What type of harm? Whatever suits the objectives the employee is trying to achieve. A recent example was an employee working from home that saw an opportunity to retain data that was not owned by them, ***but owned by the business***. Why? The data had have financial value (Trade Secrets)

This increased demand for teleworking, inter-connectivity and instant access to data, requires ***2 critical components***; **1)** Secure use of technology **2)** Visibility of employee activities on remote computer systems.

Best Practices For Teleworking

Listed below are some best practices that should be addressed for employees' who will be working from home.

- ☐ A business can't protect their data, if they don't know what they have, were it is stored, who is accessing the data, and why. Conducting a data inventory is crucial for robust data protection. What business data is stored on business owned electronic devices such as; network servers, desktop computers, laptops, tablets and smartphones?

- ☐ What business data is stored on employee' personal electronic devices?

- ☐ Do business owned computer systems that will be accessed remotely by employees', contain a Network Acceptable Use Agreement / Warning Banner?

- ☐ If the employee is using their personal home computer, does the business have a Telework Policy (Examples On Page 4) that clearly states what security practices must be taken to protect the computer and the company's data. (**Example**: Patching Of Operating System / Applications, Firewall & Anti-Virus / Malware Software, Use Of Home / Public Wifi, Use Of; VPN, Encryption Software, Etc.)

- ☐ An employee may consider working from a local coffee shop or restaurant at various times during the day, to get out of the house. If the employee is using their personal laptop computer, in addition to the above security practices, it is not recommend to use public wifi hotspots, unless a VPN is being used that will encrypt data transmissions.

- ☐ If the business data is not being stored in the cloud, what are the security practices for storing the data on employees' home or personal laptop computers? (**Example**: Encryption Software)

- ☐ An employee should never leave a company owned or employee owned laptop (Containing Company Data) computer in their vehicle.

- ☐ No one other then the employee should be using the company owned computer.

- ☐ Use Two-Factor Authentication for connecting to the company network if available.

- ☐ Encryption should be used on any portable storage devices that store business data.

- ☐ If possible, limit the access an employee has to sensitive company information, to the minimum needed to perform their job, while working from home.

- ☐ Web browsers have the capability to store passwords for access to websites. Employees' should not use the "Save Password" functions that are available in most web browsers.

- ☐ Another security risk web browsers pose is browser extensions. Employees' should not be installing unauthorized web browser extensions on company supplied computers. The other risk is web browser extensions already installed on employees' personally owned computers, used for work purposes.

- ☐ Are your employees' trained on how to detect e-mail phishing attacks? This is crucial to reduce cyber threats to your company's data and networks. These e-mail phishing attacks have already started to materialize since the beginning of the virus outbreak.

- ☐ Never send very sensitive business information to anyone requested by e-mail, no matter how urgent the request, without making a phone call to ensure this is a legitimate business request.

- ☐ Another security risk is an employee using collaboration software such as; Go To Meeting, Zoom, Microsoft Teams, etc. to share company documents with other non-company individuals, that is not authorized.

- ☐ In the event an employee who is working from home separates or is terminated from the business, how will this be handled and coordinated with; Security, Supervisor, Human Resources, IT Department, Etc.

Possible Employee Risks From Working At Home On Non-Employer Computers

- ☐ No Visibility Of Employees' Actions On Computer
- ☐ Saving Documents To Non-Business Owned Electronic Devices
- ☐ Sending Documents To Unauthorized Individuals
- ☐ Printing / Retaining Business Documents At Home (What Is The Employee Printing?)
- ☐ And Many More.....

Maintaining Employee Visibility While Teleworking

Data is figuratively a living entity. Each juncture of the data lifecycle has different security needs, and carries different levels of risk. These risks can be addressed through a mix of policy, people and technology. Managing these risks has traditionally been managed within the network and behind the firewall.

But now with the new unfortunate norm of teleworking, the network perimeter has disappeared, and businesses face the risk of loosing visibility of 3 critical parts of the data lifecycle (Creation, Storage, Movement)

Retaining the visibility of the storage and movement of data is crucial when data is being stored in the cloud, on portable storage media, mobile devices and transmitted via e-mail and through other methods.

A solution that I have thoroughly tested and used for my business to maintain visibility of our employees' on computers and networks, are solutions for employee monitoring from Veriato. There are other solutions available, but after extensive research I found the Veriato solutions were the most affordable and offered the greatest visibility for employee monitoring.

Veriato Vision (For Up To 100 Employees') (Starting At $12.50 Per Month)
Vision employee monitoring software lets you record and comprehensively track all of your employees' digital activity.

You get granular control over what activities and programs you monitor. Once the software is deployed on the company's PCs, MACs, and Androids, you can remotely monitor by department, group or individual. Additionally, you can monitor employees' that are off network or working remotely.

Vision is cloud based so there's no hardware to buy, making deployment simple and fast. You can run Vision in stealth mode, making it imperceptible to the end user. Vision Website / Data Sheet

Veriato Cerebral

Cerebral is an AI-powered security platform that integrates User & Entity Behavior Analytics (UEBA) with User Activity Monitoring (UAM), allowing rapid Data Breach Response (DBR). Cerebral Website / Data Sheet

Veriato Contact Information

sales@veriato.com
1-888-598-2788

Reducing Employees' Susceptibility To E-Mail Phishing Attacks

Another security tool I use and highly recommend is the KnowBe4 Simulated E-Mail Phishing Attack Tool. KnowBe4 is the leading provider for simulated e-mail phishing testing. KnowBe4 offers testing for up to 100 employees' for FREE. Did you know that 91% of successful data breaches started with a spear phishing attack? This tool will inform you how many employees' took the bait and clicked on a link. Just once click of the mouse is all it took to erase the data on 35,000 computers at the Saudi Aramco Oil Company in 2013.

Free E-Mail Phishing Testing

E-Mail Phishing Testing Information / Pricing

Guidance For Telework Security
SANS: 5 Steps To Securely Work From Home

NIST SP 800-46 Revision 2: Guide To Enterprise Telework, Remote Access, Bring Your Own Device (BYOD) Security (2016)
For many organizations, their employees', contractors, business partners, vendors, and/or others use enterprise telework or remote access technologies to perform work from external locations. All components of these technologies, including organization-issued and bring your own device (BYOD) client devices, should be secured against expected threats as identified through threat models. This publication provides information on security considerations for several types of remote access solutions, and it makes recommendations for securing a variety of telework, remote access, and BYOD technologies. It also gives advice on creating related security policies. (Download)

NIST SP 800-114 Revision 1: User's Guide To Telework And Bring Your Own Device (BYOD) Security (2016)
Many people telework, and they use a variety of devices, such as desktop and laptop computers, smartphones, and tablets, to read and send email, access websites, review and edit documents, and perform many other tasks. Each telework device is controlled by the organization, a third party (such as the organization's contractors, business partners, and vendors), or the teleworker; the latter is known as bring your own device (BYOD). This publication provides recommendations for securing BYOD devices used for telework and remote access, as well as those directly attached to the enterprise's own networks. (Download)

Telework Policy And Procedure Guidance
The following links may be useful for developing a telework policy for your business.
SANS Remote Access Policy
Montgomery County Maryland Program Policies & Procedures
U.S. Department Of Commerce Unclassified System Remote Access Security Policy And
National Institutes of Health Remote Work Guide
Harvard Telework Home Office Safety Checklist
U.S. Government Telework Guidance
U.S. Government Telework Safety Checklist
DoD Telework Policy

Additional Security Policies To Support Tele-Working
The polices listed below can be separate or combined into a Tele-Working Policy and Procedures document:
- ☐ Employee Acceptable Use Policy
- ☐ Internet Usage Policy
- ☐ BYOD Policy
- ☐ Data Management Policy
- ☐ Encryption Policy
- ☐ Password Policy
- ☐ Hardware / Software Configuration Standards for Remote Access To The Company 's Network

Cyber Security Awareness Training
Cybersecurity And Infrastructure Security Agency
Avoiding Social Engineering And Phishing Attacks

Defense Information Systems Agency
Phishing Awareness
Cyber Awareness Challenge

About The Insider Threat Defense Group (ITDG)
Company / Training Recognition & Endorsements

The ITDG is considered a ***Trusted Source*** for Insider Threat Mitigation training and consulting services to the: U.S. Government and companies such as; Microsoft Corporation, Walmart, Tesla Automotive Company, Dell Technologies, Symantec Corporation, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more.

The ITDG has provided training and services to over **600+** organizations. Over **780+** individuals have attended our ITP Development -Management Training Course and received ITP Manager Certificates. Client Listing

Our training courses and consulting services have been recognized, endorsed and validated by the U.S. Government and businesses, as some of the most affordable, comprehensive and resourceful available. These are not the words of the ITDG, but of our clients. ***Our client satisfaction levels are in the exceptional range.*** We encourage you to read the feedback from our clients.
Client Comments

Please contact the ITDG with any questions regarding data security, teleworking or to learn more about the Insider Threat Mitigation training and consulting services we offer.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program Development / Management Training Course Instructor
Insider Threat Vulnerability Assessor & Mitigation Specialist
Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG)
NITSIG Insider Threat Symposium & Expo Director / Organizer
888-363-7241 / 561-809-6800
www.insiderthreatdefense.us
james.henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org