# GUIDELINES FOR PREPARING PROPERTY & BUSINESS INTERRUPTION CLAIMS FOLLOWING CYBERATTACKS

**Author: Jason Conley,** Digital Forensics Examiner, Envista Forensics, Toronto

Since 2007, the frequency and impact of cyberattacks have grown exponentially, with forecasts predicting up to $10.5 trillion USD in cybercrime losses annually by 2025[1]. When a business experiences one of these immensely damaging attacks, it is vital to respond quickly. Often, businesses are so focused on recovery that they fail to take the appropriate steps necessary to ensure that they preserve sufficient evidence for analysis and compile comprehensive documentation to support their proof of loss in an insurance claim.

This whitepaper provides three crucial best practices to follow while preparing for a cybercrime claim, as applicable to property insurance claims and, sometimes, business interruption claims. Using these guidelines and considerations will assist in minimizing damages and quickly restore essential networks, systems, and intellectual data.

## RECORDING SYSTEM ACTIVITIES

While preparing documentation and recording all activities performed during the remediation of the affected systems, these records should be separated into specific categories. Details of all affected systems that will be repaired, restored, reimaged, rebuilt or replaced are pertinent information for records including:

- Make and model
- Serial number
- Operating system
- System functions
- System identifiers (i.e., internal asset tags, designated system name)
- Storage capacity, and if applicable, RAID configurations
- If the system is a virtual machine, identify it as such, and indicate on which host it resides
- If the system is infected, crypto-locked with ransomware, or both

When performing system hardening or restoration, it is important to record the following:

- **When** the work was performed, including start to finish dates and times.
- **Who** performed the work, including name, company, and position. If internal, provide whether the employee is salary or hourly, exempt or non-exempt, and whether they incurred overtime. If they are not salary, indicate their hourly rate and overtime rate.
- **What** they did and differentiate between what was replaced versus new additions (i.e., restored a bare-metal image or system snapshot, re-installed software, installed new security controls, or made

[1] 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends (2021 EDITION), Andra Zaharia, Comparitech, https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

firewall modifications).
- **How** long it took.
- **Why** was the system remediated. This could be becuase it was encrypted with ransomware, infected with malware, or the operating system is being replaced because original was incompatible with new security controls being rolled out.

## *System Restoration Records*

Property-related insurance coverage is designed to return the insured to a pre-loss condition.  Therefore, the insured must accurately document all work performed to restore a system to its original state.  Often, returning to the previous state is an undesirable pursuit, especially if this was the first significant loss event that the organization has experienced.  Some important distinctions to make while preparing these records are ensuring the separation of activities designed to restore what was in place before the loss from further changes and additions intended to enhance the systems.

Ask yourself the following questions to determine what should be included in these records:

- ***Is this task designed to bring a system back to the way it was before?***
- ***Is this task designed to recreate something that is now unrecoverable from backups or decryption?*** Some specific policy wording addresses data recreation.  For example, the recreation of diagrams, a database, or manual data re-entry.
- ***Is this task about making temporary changes?*** Temporary changes can include changing passwords, blocking ports, and adding endpoint detection and response (EDR) agents that prevent damage while the threat is still present.  Think about this carefully, some policies make room for threat containment measures, but this is only applicable if a direct threat is still present and not mitigated by other measures.  Many purchases and services that advance the security posture of the insured are viewed as betterments to the pre-loss condition, hence the need for detailed record keeping to make this distinction.
- ***Is this task specifically intended to strengthen the security posture of the organization permanently?*** Examples of permanent security strengthening tasks could include adding a firewall, network segmentation, or adding multi-factor authentication technologies.  If the answer to this question is yes, this record should not be included in this section.  Instead, this should be included in system hardening activities.

## *System Hardening Activities*

In response to cybercrimes, businesses naturally perform various changes to implement more protection. This work is referred to as system hardening and entails thoroughly examining and closing all potential access points.  All vulnerable points are identified and eliminated during this process in computer software applications, operating systems, firmware, databases, networks, and other elements that can be exploited.

All work performed to harden a system or network, add security controls, or investigate causes should be recorded separately from the processes required to restore the systems and services operational at the time of the loss, whether it is covered or not by the insurance policy.  Hardening activities include:

- Auditing your existing systems
- Consultations and time invested in determining system hardening strategies
- Patching vulnerabilities

- Firewall reconfiguration
- Adding encryption to network traffic and/or data storage devices
- Changing components or functions to provide better security
- Changing admin restrictions or access
- Turning off non-essential services
- Penetration testing

## ESTABLISHING PROOF OF LOSS AND RELEVANT DATA FOR A CLAIM

Crucial data to record following a cyberattack is adequate proof of your loss and data to support your claim. An organization's IT department should provide a complete listing of all systems on the network at the time of the event and a network topology diagram. If possible, this should include both a pre- and post-loss topology.

As part of the claim supporting data, a copy of the incident report outlining the investigation, results, and recommendations should be obtained from the digital forensics incident response providers. If ransomware was involved, copies of the ransom note, encrypted sample files, and details about the ransomware variant should be retained, this may include archived sample of the executable, hash value of the ransomware, or antivirus logs.

If this event is triggering a business interruption policy, it is important to substantiate the length of downtime the business incurred. Specific dates regarding important remediation milestones as well as substantial amounts of accounting details play an important role in substantiating the claim. It is common for a claim to be reviewed by both a data loss consultant and forensic accountant working together.

One of the most important documents to provide the adjuster and data loss consultant is the master log created at the onset of the incident and updated daily throughout the incident, including the remediation period. This typically breaks down all the affected departments, systems, and services, lists and prioritizes all the compromised systems, and updates at the end of each day. Retaining a copy of each version of this document enables future auditors to understand any delays, problem areas, or systems that took longer times than average to restore. This will be useful in both property and business interruption claims.

If a particular vendor or service provider was unable to meet reasonable expectations or was negligent in any significant portion of their commitments, document this.

## PROVIDE DOCUMENTATION TO VENDORS, SERVICE PROVIDERS, AND SUPPLIERS

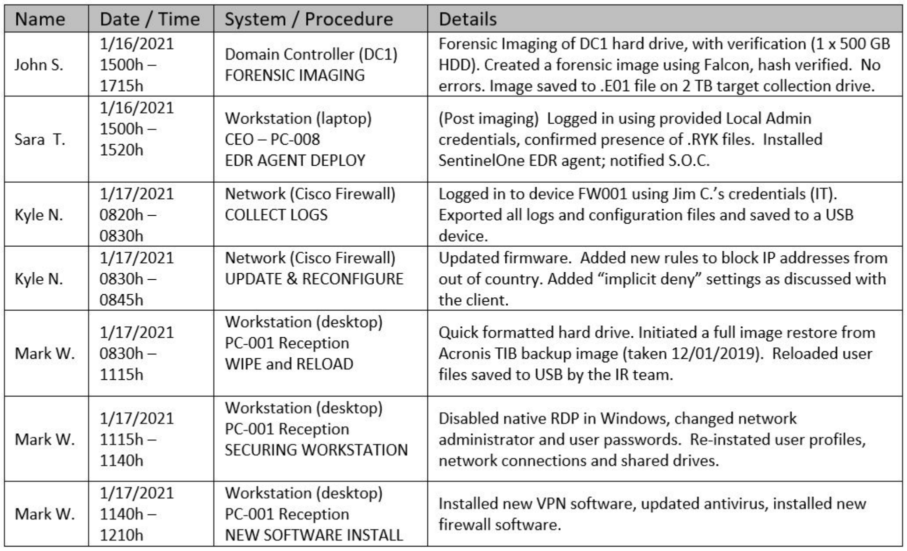
When it comes to cybercrime remediation, specific steps make the claims process more manageable. First, a formal statement of work or service agreement should be received from each vendor that provides services directly related to remediation. If a specialized vendor is required to restore an impacted system, be sure to ask them to make every effort to restore the system as efficiently as possible and return the system as close to the pre-loss condition as possible. If they are unable to do so for some reason, ensure that they come as close as possible and provide a detailed explanation for why returning the system to pre-loss was not possible. In some instances, the insured's systems may be seriously outdated, and the specialized software or hardware may no longer be available for outdated systems. If the insured wishes to choose the latest versions, the service provider can provide two quotes, one for the bare minimum system as close to pre-loss as possible and another for the system decided upon.

If changes or upgrades are required, ask the vendor to separate the time required to restore the system versus provide the upgrades. Ask all vendors to present a detailed breakdown of services provided and to record all the exact details that would be documented had they been an internal employee.

If possible, set the expectation for invoices to distinguish between the types of services provided. For example, separate restoration services, investigative services, security hardening exercises, and new installations. Failing to do so can cause speculation regarding how long was required for each activity and may result in a less desirable outcome should a claim review be performed.

If hardware is purchased, explain what it was used for and why it was purchased. Provide an overview of upgrades already underway or if plans for an upgrade were expedited because of the loss. If new security controls were being implemented that require "newer" equipment, explain why the impacted system would not support the new security controls. If specialized equipment is purchased due to a required hardware upgrade, be prepared to explain why, and provide supporting documentation.

If new software is purchased, explain why. Software license keys are usually recoverable from the registry of impacted computers, despite the presence of viruses or malware, including ransomware. If annual subscriptions or licenses are being purchased, provide supporting documentation from the previous purchase and explain why this purchase was required and was not recoverable from the original system. If this software is proprietary to a specific vendor, such as software used in industrial SCADA systems, or medical devices, provide the service agreement and ask the service provider to replace the same version of the software as before the loss event. If an upgrade is required, ask the vendor to provide an estimate for both scenarios and include this documentation in your claim.



| Name | Date / Time | System / Procedure | Details |
|---|---|---|---|
| John S. | 1/16/2021<br>1500h –<br>1715h | Domain Controller (DC1)<br>FORENSIC IMAGING | Forensic Imaging of DC1 hard drive, with verification (1 x 500 GB HDD). Created a forensic image using Falcon, hash verified. No errors. Image saved to .E01 file on 2 TB target collection drive. |
| Sara T. | 1/16/2021<br>1500h –<br>1520h | Workstation (laptop)<br>CEO – PC-008<br>EDR AGENT DEPLOY | (Post imaging) Logged in using provided Local Admin credentials, confirmed presence of .RYK files. Installed SentinelOne EDR agent; notified S.O.C. |
| Kyle N. | 1/17/2021<br>0820h –<br>0830h | Network (Cisco Firewall)<br>COLLECT LOGS | Logged in to device FW001 using Jim C.'s credentials (IT). Exported all logs and configuration files and saved to a USB device. |
| Kyle N. | 1/17/2021<br>0830h –<br>0845h | Network (Cisco Firewall)<br>UPDATE & RECONFIGURE | Updated firmware. Added new rules to block IP addresses from out of country. Added "implicit deny" settings as discussed with the client. |
| Mark W. | 1/17/2021<br>0830h –<br>1115h | Workstation (desktop)<br>PC-001 Reception<br>WIPE and RELOAD | Quick formatted hard drive. Initiated a full image restore from Acronis TIB backup image (taken 12/01/2019). Reloaded user files saved to USB by the IR team. |
| Mark W. | 1/17/2021<br>1115h –<br>1140h | Workstation (desktop)<br>PC-001 Reception<br>SECURING WORKSTATION | Disabled native RDP in Windows, changed network administrator and user passwords. Re-instated user profiles, network connections and shared drives. |
| Mark W. | 1/17/2021<br>1140h –<br>1210h | Workstation (desktop)<br>PC-001 Reception<br>NEW SOFTWARE INSTALL | Installed new VPN software, updated antivirus, installed new firewall software. |

Sample Timesheet Documentation for Employees or Vendors

Following a cyberattack, recording each task separately in timesheets and subsequent invoices can reduce the time required for the claim review and increase the speed at which the claim can be processed, in addition to helping ensure that the policy covers as much as possible and eliminate any need for speculation about the time required to execute the tasks and the reasonable value associated with each task.

When business interruption is also a factor and with the rising potential for another cyberattack during the remediation process, an experienced digital forensics team can assist with getting your security back intact, while creating and maintaining thorough records to speed up the claim.

Envista's global team of digital forensic experts have industry-leading expertise to quickly respond to all types of cyberattacks. Our experts will help you secure your systems, preserve data and evidence, and build records throughout every stage of the process, ensuring the claim is processed promptly.