Legal Pitfalls to Avoid in Security Incidents

Nick Merker, Partner, Ice Miller LLP

(@nmerker, Nick@IceMiller.com, https://www.linkedin.com/in/nickmerker/)

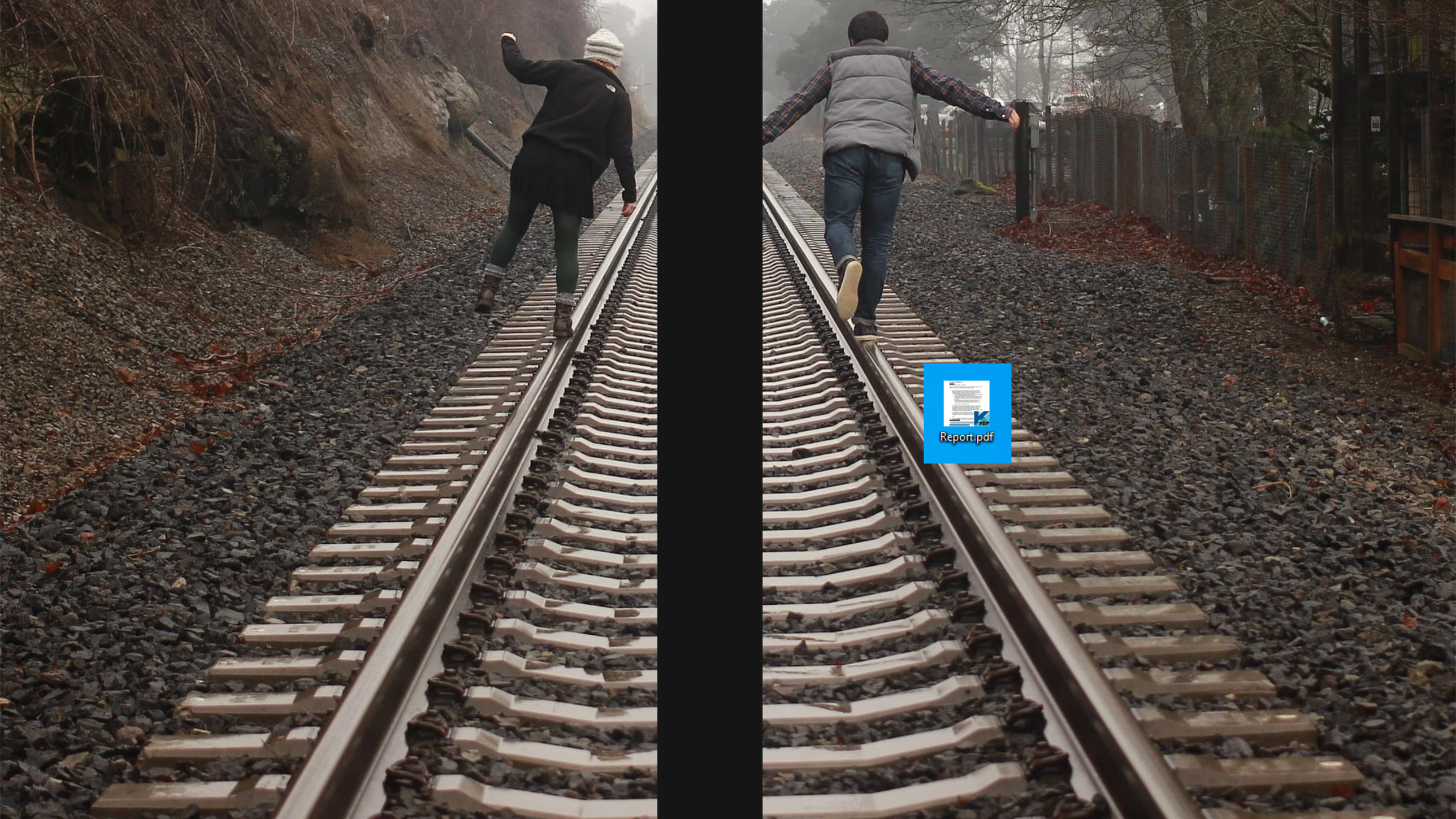
Who is this lawyer and why is he here?

Agenda.

What is Attorney-Client Privilege?

For the work product doctrine to apply, the document must be prepared "in anticipation of litigation." Fed. R. Civ. P. 26(b)(3). A document is prepared in anticipation of litigation if "in light of the nature of the document and the factual situation of the particular case, the document can fairly be said to have been prepared or obtained because of the prospect of litigation." *Martin v. Bally's Park Place Hotel & Casino*, 983 F.2d 1252, 1258 (3d Cir. 1993) (quoting *United States v. Rockwell Intern.*, 897 F.2d 1255, 1266 (3d Cir. 1990)). Aiding in "identifiable" or "impending" litigation must have been the "primary motivating purpose behind the creation of the document." *United States v. Rockwell Intern.*, 897 F.2d 1255, 1266 (3d Cir. 1990); *Leonen v. Johns-Manville*, 135 F.R.D. 94, 97 (D.N.J. 1990). To determine whether "the prospect of litigation" is the purpose behind the document, the initial inquiry is

How we investigate security incidents today.


Report.pdf

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION) MDL No. 1:19md2915 (AJT/JFA)

This Document Relates to CONSUMER Cases

GUO WENGUI, Plaintiff,
v.
CLARK HILL, PLC, et al., Defendants.

Civil Action No. 19-3195 (JEB).

United States District Court, District of Columbia.

January 12, 2021.

MEMORANDUM OPINION

JAMES E. BOASBERG, District Judge.

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA

IN RE RUTTER'S DATA SECURITY BREACH LITIGATION

CIVIL ACTION NO. 1:20-CV-382

(JONES, J.)
(MEHALCHICK, M.J.)

No Privilege for Computer Forensics Report

Plaintiff Guo Wengui has moved to compel Defendant Clark Hill, PLC, his former law firm, to produce "all reports of its forensic investigation into the cyberattack" that led to the public dissemination of Mr. Guo's confidential information. See ECF No. 25-1 (Mot.) at 3; see generally Guo Wengui v. Clark Hill, PLC, 440 F. Supp. 3d 30 (D.D.C. 2020) (discussing Plaintiff's allegations). He also asks that the Court mandate that Defendant provide more complete answers to certain interrogatories regarding its investigation into the hack. See Mot. at 3.

In light of the record before the Court, including the Duff & Phelps Report itself (which the Court has reviewed *in camera*), Clark Hill has not met its burden to show that the Report, or a substantially similar document, "would [not] have been created in the ordinary course of business irrespective of litigation." Banneker Ventures, 253 F. Supp. 3d at 72. For many organizations, surely among them law

Papered Privilege Isn't Enough

In sum, although engagement letters dated September 14 state that Clark Hill hired MPG in anticipation of litigation and that, on the same day, MPG in turn retained Duff & Phelps, Duff & Phelps's role seems to have been far broader than merely assisting outside counsel in preparation for litigation. Although Clark Hill papered the arrangement using its attorneys, that approach "appears to [have been] designed to help shield material from disclosure" and is not sufficient in itself to provide work-product protection. Dominion Dental, 429 F. Supp. 3d at 194 (finding defendant's "conclusory statement" in affidavit that report was prepared in anticipation of litigation "rebutted by extensive evidence in the record"); Premera II, 329 F.R.D. 656, 666 (D. Or. 2019) (concluding that defendant "cannot shield [consultant forensic work] from discovery by delegating [its] supervision to counsel"); see also Allied Irish Banks v. Bank of Am., N.A., 240 F.R.D. 96, 99 (S.D.N.Y. 2007) ("That [the plaintiff] hired a law firm to `assist' in the investigation is of no moment. . . . A party may not insulate itself from discovery by hiring an attorney to conduct an investigation that otherwise would not be accorded work product protection.") (cleaned up).

It is clear from the contract between Kroll and Defendant that the primary motivating purpose behind the Kroll Report was not to prepare for the prospect of litigation. Included in the contract is a "statement of work" (SOW) which includes a description of services. (Def's 6/15 Letter, at 14). The following is included in the "Description of Services" section of the SOW: "The overall purpose of this investigation will be to determine whether unauthorized activity within the Rutter's systems environment resulted in the compromise of sensitive data, and to determine the scope of such a compromise if it occurred." (Def's 6/15 Letter, at 14).

Capital One contends that the second prong of the *RLI* test was incorrectly applied as a matter of law because the Magistrate Judge gave dispositive effect to the pre-existing SOW with Mandiant, when in fact, at Debevoise's instruction, Mandiant changed the nature of its investigation, the scope of work, and its purpose in anticipation of litigation; and as a result, "Mandiant's investigation and report would have been very different if Capital One had engaged Mandiant to investigate the Cyber Incident for *business* purposes" because, in that scenario, "Mandiant's investigation would have focused on remediation." Objs. at 18 (emphasis in original). [3]

But that contention appears hollow in light of the respective scope of services covered under the Letter Agreement and the 2019 SOW, [4] which are identical; and the Addendum [redacted]

Classic Two-Track Approach Fails

Defendant, notably, does not seem to quarrel with this general thesis. Instead, it offers a more nuanced position, arguing that the Report qualifies as being prepared in anticipation of litigation because it was the result of only one half of a "two-tracked investigation of the incident." Opp. at 2. On one track, Clark Hill's

In other words, Clark Hill claims, citing In re Target Corp. Customer Data Sec. Breach Litig., MDL No. 14-2522, 2015 WL 6777384, at *2-3 (D. Minn. Oct. 23, 2015), that it had one "ordinary-course investigation" by eSentire "set up so that [it] could learn how the breach happened and . . . respond to it appropriately" — which did not result in protected work product — while it also engaged a "separate team" to "inform[] [its] counsel about the breach so that [they] could provide . . . legal advice and prepare to defend the company in litigation." Id. (finding "information generated along [the latter] track" to be protected work product). Under the Target court's approach, the latter investigation and report would apparently not have existed but for the prospect of litigation, even as the other report would have been prepared "in the ordinary course of business." In re Sealed Case, 146 F.3d at 887 (citation omitted). Ergo, says Clark Hill, it has appropriately disclosed eSentire's work and held on to Duff & Phelps's.

The problem for the defense here is that its two-track story finds little support in the record. The firm offers no sworn statement averring that eSentire conducted a separate "investigation" with the purpose of "learn[ing] how the breach happened" or facilitating an "appropriate[]" response. Target, 2015 WL 6777384, at *2. The

Sharing The Report

There is more. Hood himself admits that the Report was shared not just with outside and in-house counsel, but also with "select members of Clark Hill's leadership and IT team." Opp. at 6 (citing ECF No. 29-27 (Declaration of Edward J. Hood), ¶¶ 5-6). Hood further avers that the Report was used to "assist[] [Clark Hill] in connection with managing any issues, including" — but notably not limited to — "potential litigation . . . related to the . . . cyber incident." Hood Decl., ¶ 6 (emphasis added). Defendant also shared the report with the FBI "as part of the FBI's investigation of the cyber incident." Id. The Report was probably shared this widely, as Plaintiffs persuasively argue, because it "was the one place where [Defendant] recorded the facts" of what had transpired. See Reply at 10. There was no comparable eSentire document. The Report itself, moreover, reveals yet other ways in which Duff & Phelps worked with persons beyond MPG or Clark Hill to help the firm respond to and manage the breach.

Paper Up Privilege, But Actually Do It Too

Continue Two-Track Investigations

Use Only For Litigation Preparedness

Do Not Share Report

[redacted]

9:44 AM (0 minutes ago)

Bob, we need to deploy endpoint monitoring after this event is over. As you can see below, our lawyer is telling us he isn't sure what the threat actors did in our environment because we don't have it.

Agree?

•••

---------- Forwarded message ---------
From: **Nicholas.Merker@icemiller.com** <Nicholas.Merker@icemiller.com>
Date: Mon, Jul 5, 2021 at 9:43 AM
Subject: [redacted] Ransomware Response - Forensic Investigation
To: [redacted]

All,

Based on the forensic investigation conducted by [redacted] so far, I think there are arguments that data exfiltration did not occur. First, the root cause of the event appears to be compromised credentials used to access a single Windows server through RDP. From there, the attacker used PowerShell to move laterally across the network and deploy malware. No logs exist that show the attacker gaining interactive access to other servers to pull information off.

There is some legal risk here because we do not have a full set of logs across the environment, endpoint monitoring was not deployed, and a few other items. Let's talk this through in our upcoming meeting.

Thanks,
Nick

Nick Merker, CISSP, CIPT; *Partner*; p 317-236-2337

IceMiller
LEGAL COUNSEL

OFAC.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: October 1, 2020

OFAC.

Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations

Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA),[9] U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that causes a violation under IEEPA, including transactions by a non-U.S. person which causes a U.S. person to violate any IEEPA-based sanctions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons, which could not be directly performed by U.S. persons due to U.S. sanctions regulations. OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

OFAC.

As a general matter, OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations.[11] This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services businesses). In particular, the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction. Companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations.[12]

Under OFAC's Enforcement Guidelines, OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company's full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.

Delays at your carrier.

2. The following new definitions are added:

Ransomware Attack means the insertion of malware by a third party perpetrator on computer hardware, software or components thereof linked together through a network of devices accessible through the internet or the **Named Insured's** intranet or connected with data storage or other peripheral devices and operated by and either owned by or leased to an **Named Insured** that prevents or limits an **Insured's** ability to access data thereon for the purpose of obtaining a ransom from the **Insured** to end or remove the attack.

Ransomware Loss means those funds paid by the **Named Insured** to the perpetrators of the **Ransomware Attack** to end the attack, with the Insurer's prior approval.

Delays at your bank.

Nick:

We will need as much detail as you have available in regards to each of the items below. Once you receive this I'd recommend a conference call to digest and go through the line items so that we can discuss thoroughly.

- Amount of the payment
- Destination instructions
- Does the client have cyber-insurance – if yes, what is the name of the company
- Has the client engaged a third party vendor or intermediary to assist with negotiation or payment of the ransom - if yes, then obtain the name of company and contact information
- Confirmation from customer that a report to law enforcement was made in respect of the ransom demand/ransomware attack (e.g., IC3 report # if applicable and law enforcement agent name, if known)
- If payment through [redacted] is being considered a written representation from the client and any and all intermediaries (if any) that each have no knowledge that the ransom payment is destined for a sanctioned individual or country entity. (and the representation should explain the basis by which the party making such representation got comfortable doing so, or reached its conclusion that it does not have any basis to believe the ransom payment is being made to a sanctioned person or country).

- If the client has engaged any outside law firm to assist with the incident and who that entity is. Also, what services are they providing.
- If payment is expected through crypto-currency, who is provider, who selected them.
- A list all intermediaries that have been engaged and what their involvement/actions are.
- If there is any sort of incident response/digital forensics firm involved to help with response to the incident and who that entity is and what actions are they taking. Also, who engaged them.
- If there is an entity that will facilitate the conversion of fiat currency to cryptocurrency to pay the digital wallet of the ransomware threat actor, that entity needs to provide us with a representation that it is a federally registered money services business (MSB).

Engage outside counsel immediately.

Get crypto wallet address immediately.

Start analyzing immediately.

Actually Use Your IRP.

Actually U

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Actually U

3.2.5 Incident Documentation

An incident response team that suspects that an incident has occurred should immediately start recording all facts regarding the incident.[36] A logbook is an effective and simple medium for this,[37] but laptops, audio recorders, and digital cameras can also serve this purpose.[38] Documenting system events, conversations, and observed changes in files can lead to a more efficient, more systematic, and less error-prone handling of the problem. Every step taken from the time the incident was detected to its final resolution should be documented and timestamped. Every document regarding the incident should be dated and signed by the incident handler. Information of this nature can also be used as evidence in a court of law if legal prosecution is pursued. Whenever possible, handlers should work in teams of at least two: one person can record and log events while the other person performs the technical tasks. Section 3.3.2 presents more information about evidence.[39]

The incident response team should maintain records about the status of incidents, along with other pertinent information.[40] Using an application or a database, such as an issue tracking system, helps ensure that incidents are handled and resolved in a timely manner. The issue tracking system should contain information on the following:

- The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
- A summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, if applicable
- Impact assessments related to the incident
- Contact information for other involved parties (e.g., system owners, system administrators)
- A list of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken (e.g., rebuild the host, upgrade an application).[41]

Legal Pitfalls to Avoid in Security Incidents

Nick Merker, Partner, Ice Miller LLP

(@nmerker, Nick@IceMiller.com, https://www.linkedin.com/in/nickmerker/)