ISSA
Information Systems Security Association International

Ronald Chichester, J.D., CISA
Attorney at Law

Forensic – Tracking the Hacker

Disclaimer

- I am an attorney…
- … but I'm not *your* attorney
- If you need legal advice, hire a competent attorney (like me)
-
- If this *were* legal advice, it would be followed by a bill.

You've Been Hacked. Now what?

- Things to remember…
  - Hacking is a civil and/or criminal violation
  - All remedies for that violation require a court
  - Courts require evidence
  - Everything that you have done so far is to obtain evidence
  - If you don't have evidence that can be introduced at a trial, you don't have a case
  - No case, no remedy

What You Should Do

- The first “rule”…
  - Sue the money

What You Should Do

- The first “rule”…
  - Sue the money
- The second “rule”…
  - To sue the money, you have to figure out who has the money

What You Should Do

- The first “rule”…
  - Sue the money
- The second “rule”…
  - To sue the money, you have to figure out who has the money
- The third “rule”…
  - Figure out where the money (or the person) is

What You Should Do

- The first “rule”…
  - Sue the money
- The second “rule”…
  - To sue the money, you have to figure out who has the money
- The third “rule”…
  - Figure out where the money (or the person) is
- The fourth “rule”…
  - Make sure the case against the bad guy is better than the case against ***you***

Why the “Rules”?

- To get a remedy, you need a court

Why the “Rules”?

- To get a remedy, you need a court
- Courts require jurisdiction

Why the “Rules”?

- To get a remedy, you need a court
- Courts require jurisdiction
- Once you know in which court you can avail yourself, you can figure out which laws apply

Why the “Rules”?

- To get a remedy, you need a court
- Courts require jurisdiction
- Once you know in which court you can avail yourself, you can figure out which laws apply
- Once you know which law applies, you can see what elements must be established

Why the “Rules”?

- To get a remedy, you need a court
- Courts require jurisdiction
- Once you know in which court you can avail yourself, you can figure out which laws apply
- Once you know which law applies, you can see what elements must be established
- Once you know the elements, you can correlate the elements with the evidence to determine if you can make a case

Who Done It?

- Getting the hacker is satisfying

Who Done It?

- Getting the hacker is satisfying
  - But doesn't happen very often

Who Done It?

- Getting the hacker is satisfying
  - But doesn't happen very often
- Follow the money…

Who Done It?

- Getting the hacker is satisfying
  - But doesn't happen very often
- Follow the money…
  - In many cases, identifying who receives the benefit of the hack can lead to a case

Who Done It?

- Getting the hacker is satisfying
  - But doesn't happen very often
- Follow the money…
  - In many cases, identifying who receives the benefit of the hack can lead to a case
  - Possible to leave a trace in the documents that can lead to the target of the investigation

Civil v. Criminal

- Some hacking statutes have criminal sanctions
- Others have civil sanctions
- Some have both

Civil v. Criminal

- Some hacking statutes have criminal sanctions
- Others have civil sanctions
- Some have both
- Jurisdiction: Federal v. State
  - Federal laws, e.g., the Computer Fraud and Abuse Act (18 U.S.C. 1030)
  - State laws, e.g., Texas Penal Code Sec. 33.02
  - Texas Business & Commerce Code Sec. 48
  - Texas Business & Commerce Code Sec. 324

Additional Considerations

Additional Considerations

- Cost
  - Can your company get indemnified for the cost of the investigation and legal proceedings?
  - What are the ancillary costs to the company?
    - Executive downtime
    - Device downtime
    - Cost of gathering/storing evidence

Additional Considerations

- Cost
  - Can your company get indemnified for the cost of the investigation and legal proceedings?
  - What are the ancillary costs to the company?
    - Executive downtime
    - Device downtime
    - Cost of gathering/storing evidence
- Reputation/Publicity

Questions?

- Ronald L. Chichester, J.D., CISA
- Phone: 713-302-1679
- Email: Ron@TexasComputerLaw.com