YOUR COMPANY JUST EXPERIENCED A CYBER INCIDENT. NOW WHAT?

Jason C. Kravitz
Practice Leader, Cybersecurity & Privacy
Nixon Peabody LLP

NIXON PEABODY

IT'S FRIDAY AND YOU'RE LOOKING FORWARD TO THE WEEKEND

Then your CIO calls to tell you your company has just been hacked

Your day just got *much worse*

YOUR TEAM IS LOOKING FOR LEADERSHIP

You weigh your options…

OPTION 1

OPTION 2

OPTION 3

FIRST THINGS FIRST

The first thing you should do is call your attorney

Why your lawyer?

Because we have all the answers, right?

YOU CALL YOUR ATTORNEY

Because you want everything that follows to be **privileged**

WHY IS THIS IMPORTANT?

You may be confident that you did nothing wrong

But you never know

And it’s better to be safe than sorry

WHAT WILL YOUR ATTORNEY DO?

She will…

Consult your incident response plan

Because of course your company has one, right?

And of course it’s been updated, right?

LET YOUR ATTORNEY QUARTERBACK THE INCIDENT RESPONSE

WHAT WILL YOUR ATTORNEY DO?

She will…

Speak to your IT team and find out what they know

Tender claim to cyber insurance carrier

Line up a forensic investigator

Digest the information and advise on next steps

NEXT STEPS

Next steps will depend on the type of breach, but time is always of the essence

Insurance carrier may assume control over the response

If carrier delays, you must take steps to protect the company and its data

RANSOMWARE

If it’s a ransomware attack:

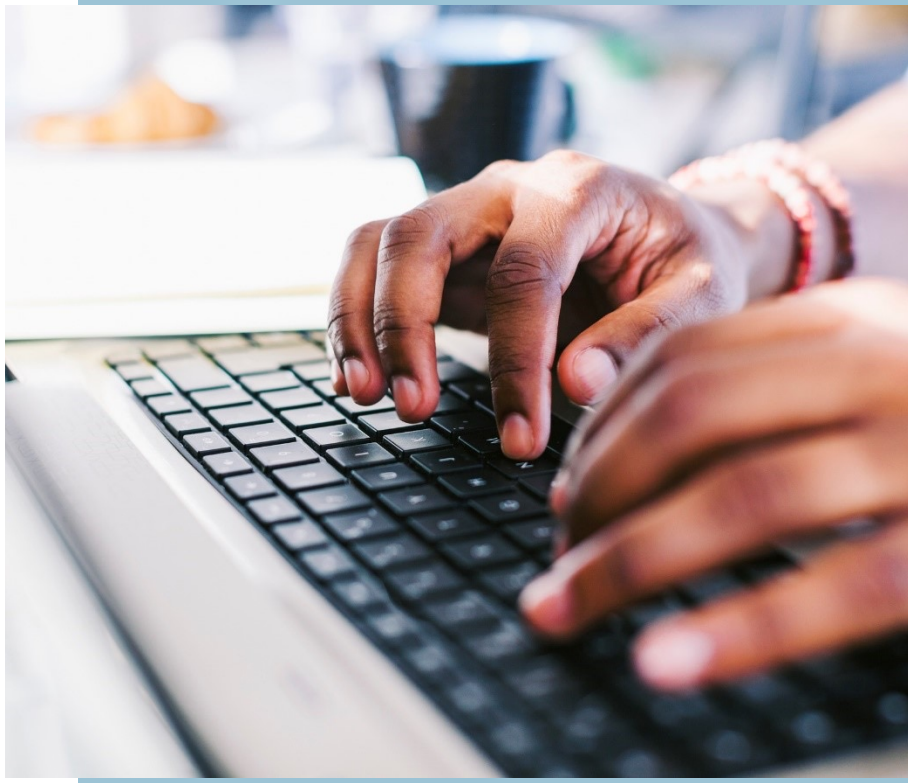
- Determine files that have been locked
- Confirm that machines have been taken offline
- Assess whether law enforcement must be notified
- Decide whether to negotiate and pay ransom

OTHER TYPES OF CYBERATTACKS

- Phishing or other social engineering attack
- DOS/DDOS attack
- Brute force attack
- DNS spoofing attack
- Trojan horse attack

OTHER TYPES OF CYBERATTACKS

- Other types of attacks may allow for more deliberative response
- Forensic security team will use software tools to assess scope of attack
- Critical to cooperate fully



NOTIFICATION OBLIGATIONS

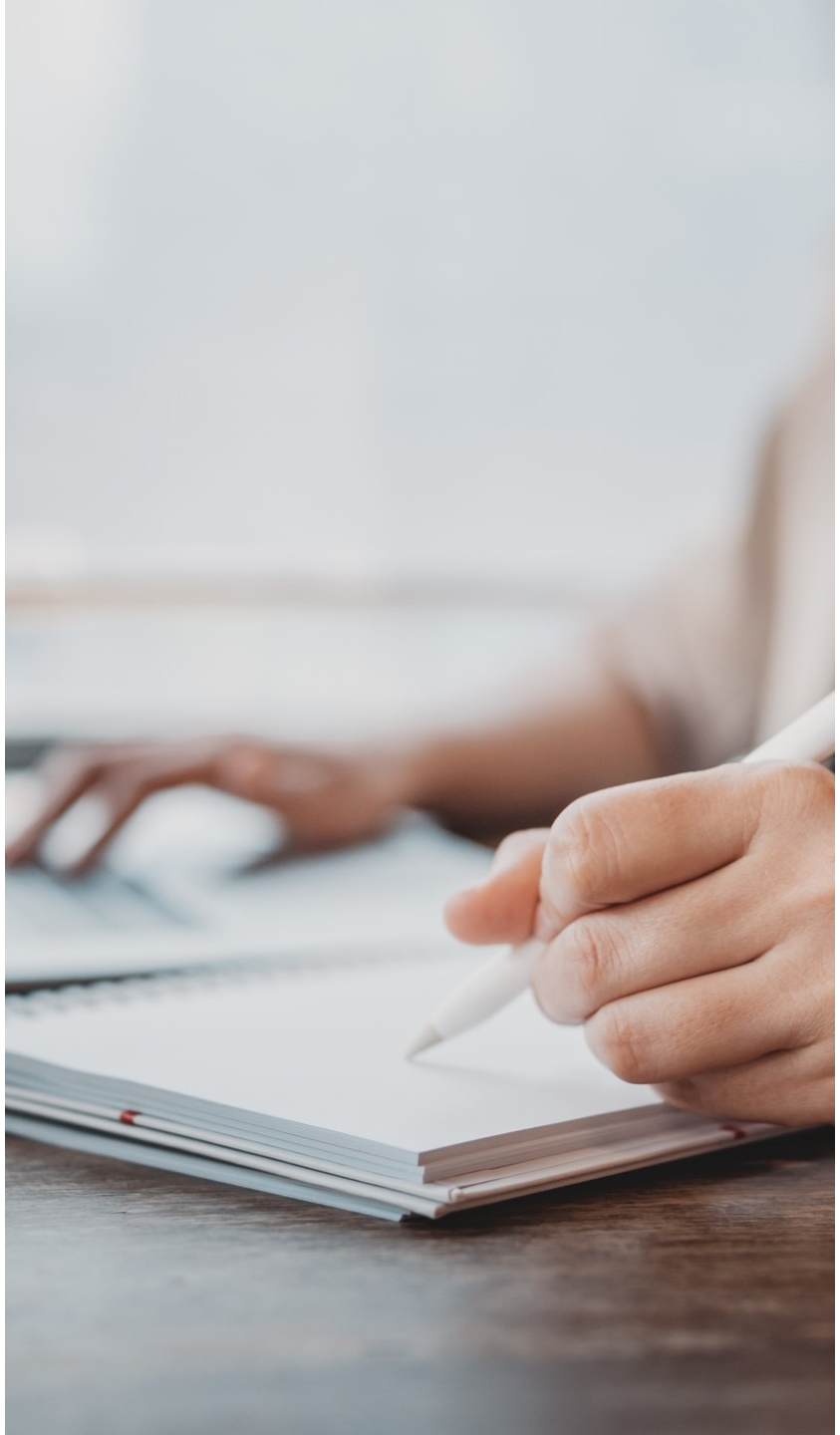
Federal and state law/regs may require notification:

- If personally identifiable information (PII) compromised
- If personal health information (PHI) compromised

Heed counsel's advice to avoid fines and to minimize risk of litigation

IMPORTANCE OF REMEDIATION AFTER ANY CYBER ATTACK

- Don’t assume the problem has been eliminated
- Allow security vendor to do their jobs thoroughly
- Get a “clean bill of health” in written report
- Not the time to cheap out



LEARN FROM YOUR MISTAKES

- Educate employees to minimize risk of recurrence
- Consider investing in more sophisticated defensive tools
- Back up as much data as you can


MAKE SURE YOUR FIRST CALL IS TO YOUR CYBERSECURITY ATTORNEY

Jason Kravitz

Partner

Practice Leader, Privacy & Technology

Boston

617.345.1318

jkravitz@nixonpeabody.com

THANK YOU