# WHAT NOT TO DO AFTER A SUSPECTED CYBER INCIDENT

In the event of a cyber incident, the instinctive response to act quickly may lead to an unsatisfactory solution. If a threat actor infiltrates one of your systems, the recommended list of what to do is nearly as long as the list of what NOT to do.

## WHEN MANAGING A CYBER INCIDENT, KEEP THESE “DON’TS” IN MIND

### DO NOT DESTROY EVIDENCE

When managing cybersecurity incidents, it is important to not destroy evidence. Some clients instinctively bring in IT providers to rebuild systems before preserving evidence, potentially leading to costly consequences, such as having to notify the entire client base.

### AVOID ARBITRARY RESTORATION

Do not restore systems to the closest available backup. Threat actors often linger in the environment for days to weeks before being detected. Restoring to a compromised state could worsen the situation.

### DO NOT CONTACT THREAT ACTORS DIRECTLY

In the event of a ransomware attack, refrain from reaching out to threat actors before seeking legal counsel or professional assistance. Consulting with a legal team can help assess the consequences of communicating with threat actors. Leave contact with the threat actor to qualified negotiators.

### AVOID HANDLING COMPLEX INCIDENTS ALONE

Do not attempt to manage a complex incident without seeking outside guidance. Managing it alone often leads to complications, as you'll likely need external assistance at some point and may have to undo previous actions. Utilize available resources, such as your data breach coach or insurance broker, for guidance.

### DO NOT USE COMPROMISED COMMUNICATION CHANNELS

Stop using your email the moment you suspect it's been compromised. Switch to more secure communication channels, such as phone calls or platforms with robust security features, like Microsoft Teams or Slack, to protect sensitive information.

### REFRAIN FROM USING THE TERM, “BREACH.”

Avoid using the term, "breach.” Instead, use the term, “security incident." A lawyer is the one to make that legal determination after analyzing forensic evidence.

### AVOID MAKING HASTY PUBLIC STATEMENTS

Refrain from making broad public statements before conducting a thorough investigation. It is essential to collect all relevant facts before communicating with stakeholders, as spreading incorrect or incomplete information can lead to misunderstanding and panic.

## LET’S TALK ABOUT PROTECTING YOU AND YOUR BUSINESS.



BRP
CYBER CENTER OF EXCELLENCE

K&S INSURANCE
A BALDWIN RISK PARTNER