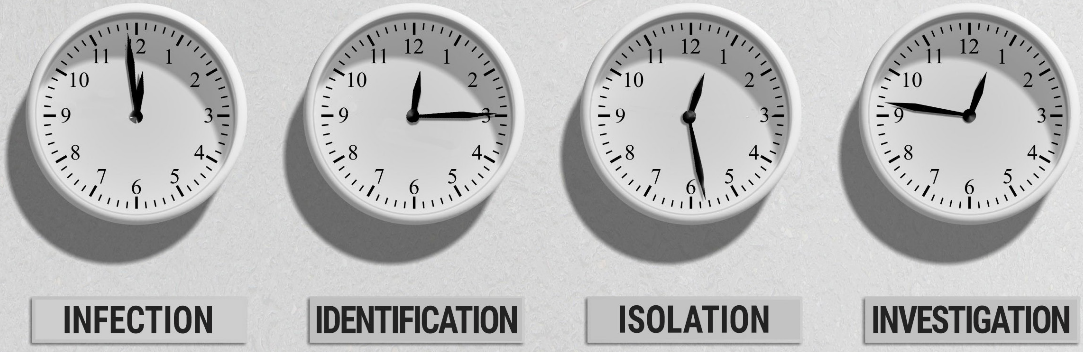
Monthly Newsletter June 2024

THE BSS ADVISOR

Business System Solutions

Caretakers of your Productivity since 1995 www.bssconsulting.com

Survive a Cybersecurity Attack!



Knowing what to do when you're hit with a cybersecurity attack can make the difference between recovery and total loss.

Photo by Pixabay/edited by awilliams, BSS

by Anisa Williams, BSS Staff

Disclaimer: these are best practice recommendations for a cybersecurity incident response. Your organization may be required to comply with certain procedures in your organization's disaster recovery plan, your business insurance policy, regulatory compliance requirements, and/or legal requirements. BSS does not take responsibility for results or outcomes.

Just like any emergency, whether small or large, actions taken in the first few minutes can drastically change the outcome of the resolution. When it comes to a cybersecurity attack, small compromises can be fixed with a password change or an MFA re-authorization. But larger compromises, up to and including ransomware, should follow similar steps, documented in an Incident Response plan, to ensure a successful recovery.

INFECTION

It's sometimes difficult to pinpoint the exact time a compromise has occurred at the time of discovery. Some hackers get into a system and squat there for months, poking around, trying to access to other systems and exfiltrating data. Others may immediately deploy ransomware or some variety of destruction on gaining access; it all depends on the type of attack and the attacker's intent.

(Continued on Next Page)

Business System Solutions is your IT Service Partner who provides peace of mind through guidance, education, and responsive support. We're the Caretakers of Your Productivity.

Serving:
North Central Indiana
(765) 742-3440

Middle Tennessee
(615) 819-0600

West Michigan
(616 776-0400

info@bssconsulting.com

"Trust in the Lord with all your heart and lean not on your own understanding; in all ways submit to him, and he will make your paths straight."
Proverbs 3:5-6

(Continued from page 1)

ZERO HOUR: IDENTIFICATION

Some of the most common breaches will not give you obvious “hey you’ve been hacked” message (ransomware). Sometimes a computer is behaving strangely or just painfully slow (malware), or you’re getting multiple MFA requests (stolen credentials).

If something seems off or wrong with your computer or network, **call IT Support immediately** so that the technician can take emergency precautions.

5-10 MINUTES: ISOLATION

- You or your IT technician should isolate the computer: on the device, **turn off Wifi and disconnect the ethernet cable but do not turn off the computer** to preserve the forensic data.
- Check other computers in the network – **repeat isolation for every device afflicted.** This may include servers, non-user or shared computers, and network storage devices.

20 MINUTES: INVESTIGATION

- Start a log of investigative activities to help define the scope of the security incident. This is critical as it’s required for both insurance and legal. Avoid using terms like hacked, breach, or attack.
- IT technicians should ensure that the backups are isolated and protected.
- Lock down accounts, tools, and active sessions.
- Audit for any unusual tasks, scripts, or policy changes that occurred. Verify all security protocols are in place and have not been disabled.

30 MINUTES: COMMUNICATION

- Notify Communication Point-of-Contact. This person may be a C-level, Director, VP, or head of Marketing or IT that will manage communication about the security incident between all parties: IT, staff, insurance, legal, law enforcement, customers, media, etc.
- Call your insurance company, legal representative/breach attorney, and law enforcement.
- Need-to-Know Only: Any information or theories about the security incident should be kept on a need-to-know basis for legal, law enforcement, and insurance reasons.

45-60 MINUTES: ASSEMBLE

- Assemble the Incident Response (IR) team: IT, communication, insurance, legal, and law enforcement. Review the investigation, discoveries, and steps taken to identify and isolate the afflicted machines.
- Staff Notification Part 1: If other users are affected by the breach, notify them that there has been a security incident and that it is being investigated – *not more than that*.
- Delegate appropriate non-technical staff to help with damage control and supporting of the technical and third-party response teams. This could include taking scheduled tasks or manning the phones, as an example.

1-3 HOURS: SITUATION ROOM

- If it’s a large-scale event, set up a conference room as a centralized situation room with critical response team members to help resolve the incident.
- Approved Talking Points: If the incident is large enough, work with the breach attorney to verify the talking points or scripts for internal and external communication.
- Staff notification Part 2: Provide those talking points or scripts to employees on how to answer questions about the incident, especially to customers/clients. Have all questions or inquiries directed to the Communication Point-of-Contact.

REMEDIATION

- Once the investigation is complete, coordinate a remediation event with the IR team & techs.
- Start the technical remediation: Change passwords, patch the vulnerable systems, remove the malicious access or code, reimage

(Continued from page 2)

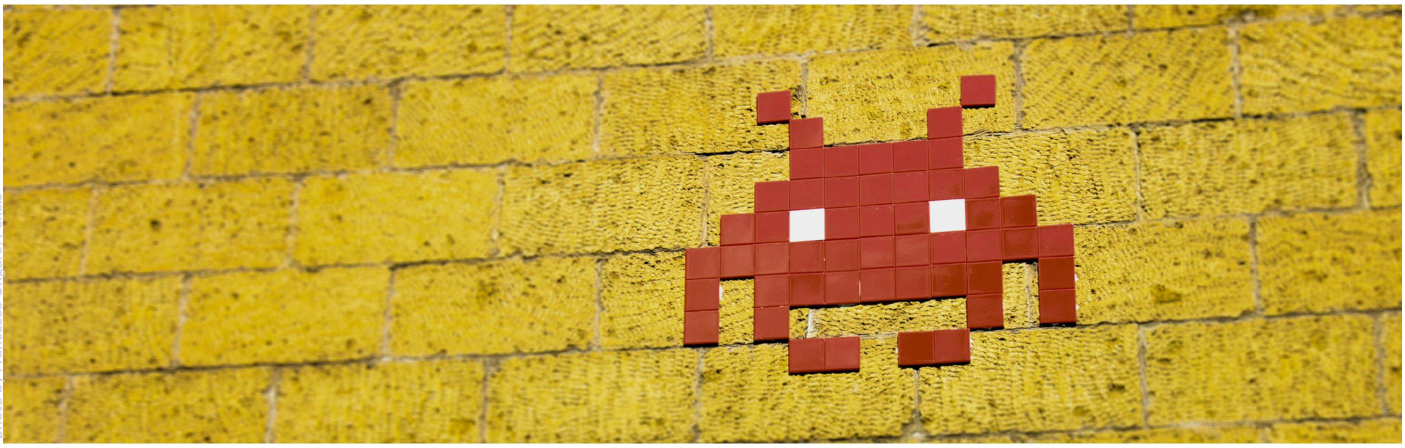


photo by Francesco Ungaro/Pexels

or remove systems, and revert to clean backups.

- Make sure the IR & tech teams have food and beverages during the remediation process as they may be experiencing long hours.
- Coordinate shifts if remediation is a multi-day event.

POST-EVENT ANALYSIS

- Work with your third-party response team to reflect on the event – good, bad, and ugly.
- Review and revise your Incident Response or Disaster Recovery Plan to reflect lessons learned.

THE DON'TS

- Don't communicate directly with the threat actor. Leave that to your third-party law enforcement or legal experts.
- Don't sacrifice forensic data in favor of restoration.
- Don't use words like breach, hack, or attack prematurely. Use the word "incident" or "security issue."
- Don't share your theories on what happened, especially before it's been confirmed. **Stating what you "think" might have happened could compromise your ability to collect on an insurance claim.**
- Don't interfere with the experts' investigation but do ask for regular updates.
- Don't post on social media or share details about the investigation or remediation while it's ongoing.

✓ THE DO'S

- Do reach out to law enforcement. They will be able to apply their considerable resources to assist, track down the threat actors, and prevent this from happening again. Most agencies involved in cybersecurity incidents are eager to help businesses of all sizes to recover well.
- Do keep your employees in the loop, especially if affects them directly, with specific updates that do not compromise the investigation.
- Do let your employees know *why* they shouldn't discuss the active investigation with customers, family, or share on social media.
- Do discuss the incident with peers, advisors, and networks **after** the situation has been resolved. Normalizing communication around security incidents can provide much-needed information to help others and provide best practices for resolution.
- Do establish relationships with the response team experts **before** a cybersecurity incident happens. You'll want them on speed dial and for them to be aware of your disaster recovery plans.

It is possible to recover quickly from cybersecurity incidents, even the very largest of ones. Recovery becomes easier when properly planned out and documented in an Incident Response Plan. Ensuring all parties know what to do and when to do it means that when a cyberattack occurs, data can be saved and business downtime minimized.

And don't turn off those computers. □

Business System Solutions

Return Address:
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544

The BSS ADVISOR

info@bssconsulting.com

North-Central Indiana Office
1211 Cumberland Avenue
West Lafayette, IN 47906
(765) 742-3440

Middle Tennessee Office
1026 West College Street
Murfreesboro, TN 37129
(615) 819-0600

West Michigan Office
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544
(616) 776-0400

2020 Winner 2021 Winner
2022 Winner 2023 Winner
Channel Futures
Leading Channel Partners Forward
MSP 501

Holiday Closures

7/4: INDEPENDENCE DAY

OnCall Support is available 24/7 during holidays.
Support emails will be handled the next business day.

Upcoming Events

Michigan 6/27, 3-5 PM

RIBBON CUTTING & OPEN HOUSE

Details at bssconsulting.com/news-events

Tennessee 7/30, 12-2 PM

MTC BACK TO SCHOOL EVENT

Details at bssconsulting.com/news-events

Know These Numbers for IT Support: 765, 615, 616

Our expert technical team is located in three different states: Indiana, Tennessee, and Michigan. Service tickets are not assigned geographically, rather by expertise so every one of our clients receives the fastest and best service.

When you reach out to us for help, **the next available technician will be assigned to your ticket.** This may mean that you'll be talking with a BSS tech in another state and **they will be calling from a 765, 615, or 616 area code.** Be assured they are from BSS!

Additionally, you can check our website for their name and photo: bssconsulting.com/about-us/our-team