Comprehensive Cybersecurity Incident Response Plan for PHCP/PVF Companies

Overview: This incident response plan is tailored for ASA members. It provides simple, actionable steps to handle various cyber threats – including ransomware, phishing, data breaches, insider threats, and supply chain attacks – and can be adapted to each organization's needs. The plan is organized by key response phases: identifying an incident, taking immediate action, containing the threat, reporting to stakeholders, recovering operations quickly, and preventing future incidents. Each section emphasizes clarity and speed, enabling non-technical staff to recognize issues and respond effectively.

Incident Identification (Recognizing a Cyber Incident)

Non-technical employees are often the first to notice something "off," so it's crucial they know the warning signs of a cyber incident. All staff should be trained to spot and **promptly report** unusual computer or network behavior. Common indicators of an attack include:

- **Unusually Slow or Erratic System Behavior:** Computers running much slower than normal or freezing frequently.
- **Access Problems:** Users suddenly being locked out of accounts or unable to open files and documents they could before.
- **Strange Messages or Pop-ups:** Ransomware notes demanding payment to unlock files, or antivirus alerts that malware was detected.
- **Suspicious Emails Sent Out:** Customers or coworkers report receiving strange or unauthorized emails from your company domain (sign of a compromised email account).
- **Browser Redirections:** Web searches or clicks consistently redirect to unfamiliar websites, indicating possible malware.
- **Unusual Requests or Transactions:** Receiving requests that bypass normal procedures – for example, urgent fund

transfer requests that turn out to be fraudulent (a sign of email compromise), or finding out about payments you never authorized.
- **Account Anomalies:** Login alerts at odd hours, or account activity that doesn't match the user's normal behavior.

If an employee observes any of these red flags, they should treat it seriously and notify the designated person or IT support **immediately**. Early reporting is vital – even a false alarm is okay. Creating a culture where staff feel comfortable escalating suspicious activity helps catch incidents early. For example, if someone receives a phishing email or their computer acts strangely, they should alert a supervisor or your IT point-of-contact right away instead of ignoring it. In many cases, multiple people may be targeted, so encouraging employees to speak up helps the whole organization respond faster.

Immediate Response Actions (First Steps for Different Attack Types)

As soon as a potential incident is identified, quick action can significantly reduce damage. Non-technical staff should focus on a few critical steps: **stay calm, disconnect affected devices from the network, and call for help.** In a small PHCP/PVF company, this likely means contacting your external IT support provider or consultant and informing a manager. Below is step-by-step guidance for common attack scenarios:

1. Ransomware Attack:

If you see a ransom message on your screen or find files encrypted and inaccessible, **assume a ransomware attack is in progress.** Take these immediate steps:

1. **Isolate the Computer:** Disconnect the infected PC from Wi-Fi or unplug its network cable at once to prevent the ransomware from spreading to shared drives or other systems. If the infection is suspected on multiple machines, consider temporarily taking the broader network offline. Only if you cannot disconnect a device, power it down as a last resort to halt the encryption process.
2. **Secure Backups:** If your company uses external backup drives or servers, make sure they are **physically disconnected** or isolated now. This prevents the

ransomware from reaching your backups (which are crucial for recovery).

3. **Notify Leadership and IT Support:** Inform your supervisor or business owner **immediately** about the situation. At the same time, contact your IT support provider or consultant and explain what happened (e.g. "We have a ransom note on our screen"). The IT experts can help assess the scope and guide next steps.
4. **Do Not Pay the Ransom (Initial Stance):** Law enforcement agencies advise against paying ransoms, because it funds criminal activity and there's no guarantee you'll get your data back. Focus on recovery steps (next sections cover containment and restoration). Only in extreme cases, after consulting experts and weighing options, would paying be considered – but the default action should be **attempted recovery via backups** rather than payment.
5. **Document Everything:** Note the time you discovered the attack and any messages or filenames associated with the ransomware. If possible, take a photo of the ransom screen with a phone. This information will be useful for investigators and for restoring data from backups.

2. Phishing Attack (Email/SMS Scam):

Phishing can either be **preventative** (you caught a suspicious email) or **reactive** (an employee fell for a scam). Respond accordingly:

- **If you receive a suspicious email or text:** Do **not** click any links or attachments. Do not reply with any information. **Report the phishing attempt internally** – forward the email to a security contact (or simply alert your manager) and delete it. By reporting it, others can be warned and filters can be updated to block similar emails.
- **If a scam email was clicked or information was given:** Take action right away:
    1. **Disconnect the Device:** If you clicked a link that might have infected your computer with malware, unplug the network connection or turn off Wi-Fi immediately. This limits any malware from communicating out or spreading.
    2. **Change Credentials:** If you entered a password on a fake site or suspect your email credentials were stolen, **change those passwords immediately** (from a different, clean device if possible). For a potentially compromised email account, also enable multi-factor authentication if it wasn't already on, to lock out the attacker.

3. **Notify IT and Management:** Let your IT support/provider know exactly what happened (e.g. "I clicked a link in a suspicious email and entered my email login before I realized it was fake"). They may need to check logs for any unauthorized access and scan your machine for malware. Also inform your supervisor so the company is aware of a possible breach.
4. **Alert Colleagues if Needed:** Phishing attacks often target multiple people. If you fell victim, quietly alert any colleagues who might have received a similar message so they don't fall for it too. For example, if you clicked a bogus invoice email, others in accounting might have that email as well – warning them prevents further harm.
5. **Contact Relevant Third Parties:** If the phishing led to sensitive info being sent (e.g. you forwarded a client list or payment info), notify those affected third parties through the proper channels. For instance, if a scam impersonated your supplier or bank, contact that organization to inform them of the phishing scheme.
6. **Report the Phish Externally:** After containing the immediate risk, you can formally report the phishing attack. Forward the phishing email to authorities like the FTC (at **spam@uce.gov**) and the Anti-Phishing Working Group (**reportphishing@apwg.org**). This helps law enforcement track phishing trends. (This step can be done by management or IT on behalf of the company.)

3. Data Breach:

A data breach is suspected when sensitive company or customer information is believed to be stolen or exposed without authorization. This might be discovered through an external alert (e.g. law enforcement or a partner says your data is online) or internal signs (unusual database activity, lost device, etc.). Here's how to respond immediately:

1. **Secure and Isolate Affected Systems:** If the breach involves a specific server, database, or computer system, take it offline from the network to stop any ongoing data exfiltration. For example, if a file server is suspected of leaking data, disconnect it from internet access or unplug it entirely. If an employee laptop with sensitive data was stolen, remotely lock or wipe it if your tools allow.

2. **Change Access Credentials:** Assume the attacker may have compromised passwords or keys. **Reset passwords** for any user or system accounts that were involved in the incident (especially if an admin account or an email account was hacked). Disable any user accounts that appear to have been used in the breach until they can be reviewed. This helps cut off the intruder's access.
3. **Preserve Evidence:** Do not immediately wipe or "clean up" the systems – first, preserve logs and evidence. If you have an IT support or incident response team, they will need system logs, access records, or even copies of affected systems to determine what happened. If you're not sure how to do this, simply avoid tampering with the system beyond what's needed to stop further damage (for instance, don't delete files or logs).
4. **Inform Management and IT Support:** As with other incidents, notify the appropriate internal lead (owner/manager) and your external IT experts right away. Provide any details you have, such as how you discovered the breach and what data might be affected. This will prompt a deeper investigation. **Containment and impact assessment** are critical in the early moments of a breach.
5. **Initial Triage of What Was Stolen:** If possible, quickly assess what type of data is involved. (Your IT partner or consultant can help with this analysis.) Determining whether the breach includes personal customer info, financial records, passwords, etc., will guide the next steps, especially reporting and notification requirements. For example, losing personal identifiable information (PII) like customer addresses or credit cards typically triggers specific legal notifications – whereas an internal-only data exposure might be handled differently. Prioritize understanding the scope: how many records or what systems are involved.
6. **Short-Term Containment Measures:** Depending on the situation, you might deploy quick fixes: for instance, apply a known security patch if the breach occurred through an unpatched vulnerability, or block certain network traffic if data was being sent out of your network. These are technical steps your IT support can guide. The goal is to **stop the bleeding** – ensure no more data is leaving the organization while you plan a fuller remediation.

4. Insider Threat Incident:

Insider threats involve a malicious or negligent insider (employee, contractor, etc.) who is harming the company's cybersecurity.

These can be hard to detect, but if you **suspect an insider is stealing data or sabotaging systems**, act with care and urgency:

- **Discreetly Involve Leadership and HR:** Immediately report your concerns to a trusted manager or executive. Given the sensitive nature, this might involve senior management, HR, and possibly legal counsel working together. Do **not** confront the suspected insider directly or accuse them publicly. Instead, elevate the issue through proper channels. For example, if you observe a coworker copying large amounts of confidential files to a personal drive without need, quietly inform your supervisor or HR **without alerting that coworker**.
- **Limit the Person's Access (If Authorized to Do So):** If you have the authority or support to take action, consider **temporarily disabling the user's computer accounts or access cards** to prevent further damage. This should be done in coordination with management/IT – typically, an IT admin or external IT provider would be instructed to revoke the individual's credentials and access rights while an investigation is underway. The principle is to **isolate the threat** just like with a virus: in this case, by cutting the insider's digital access to systems and facilities.
- **Preserve Logs and Evidence:** Ask IT (or your external provider) to save relevant system logs, access records, CCTV footage (if physical access is involved), or any forensic data related to the insider's activities. This evidence is crucial for any internal disciplinary action or law enforcement investigation. For example, if the insider is suspected of leaking customer lists, ensure email logs or file access logs are secured for review.
- **Engage Law Enforcement if a Crime Occurred:** Remember that certain insider actions (theft of data, intentional damage to systems) are crimes. Companies are encouraged to report criminal incidents to law enforcement. If you have clear evidence of malicious insider activity (such as an employee intentionally destroying data or stealing trade secrets), involve the police or FBI as appropriate. **Do not hesitate out of embarrassment** – reporting not only helps potentially stop the perpetrator but could also protect other companies from the same individual. In one real example, a company that discovered an IT admin was sabotaging systems reported it, and the employee was later arrested and charged. Always prioritize safety: if an insider threat also poses a physical danger or violent behavior, contact law enforcement immediately.
- **Internal Communication Control:** While the incident is under investigation, instruct staff *on a need-to-know basis*. Rumors can spread fast in a small company, so have

management communicate carefully. They might say, "We're experiencing a security issue and taking precautionary measures, please bear with us," without naming the individual, until official action is taken. This ensures others remain vigilant (in case the person tries something else) but doesn't unduly defame anyone before facts are confirmed.

5. Supply Chain Attack:

A supply chain attack occurs when a partner or vendor that your business relies on is compromised, leading to a potential impact on your systems. This could be a software supplier (for example, a compromised software update) or an IT service provider breach that cascades to you. Responding to a supply chain incident involves coordinating with external parties:

1. **Identify the Scope for Your Company:** As soon as you learn that a vendor or product you use has been breached, determine which of your systems or data might be affected. For example, if a popular HVAC control software used in your warehouse announces a malicious update, check if you installed that update. Or if your cloud service provider was hacked, find out which of your data or services could have been exposed. This may involve contacting the vendor for clarification and following any advisories they provide.
2. **Isolate or Shut Down Affected Services:** Treat the compromised third-party system as if it were infected in your own network. **Isolate it from the rest of your environment.** For instance, if it's a software tool, temporarily stop using it or disconnect it from your network until it's verified safe. If an IT service provider (like a managed IT company) is breached, consider disabling their remote access to your systems until you can confirm your systems are secure. This containment step prevents the supplier's issue from doing more harm to your business.
3. **Apply Patches or Mitigations:** Often, when a supply chain attack is discovered, the vendor or authorities (like CISA) will release guidance or patches. **Follow the recommended steps** immediately – e.g., apply security patches, revoke compromised certificates or credentials, or run specialized detection tools to find indicators of compromise. Your external IT support can help with this. The goal is to remove or neutralize the compromised component of the supply chain attack.
4. **Communication with the Vendor:** Stay in close contact with the affected supplier. Confirm that they are addressing

the issue and ask for updates on what went wrong and what data (if any) was accessed. If the vendor provides a timeline of the breach or specific data that was taken, use that to inform your own next steps (such as notifying customers if their data was involved).

5. **Assess Data Exposure:** If the supply chain attack involved a third-party that holds your data (for example, a cloud CRM provider or an external payroll service), work with them to understand what information of yours might have been compromised. This may feel frustrating as you rely on them for answers, but push for clarity: ask "Did the attackers access our company's records? Which ones, and when?" This information will determine if you need to enact your data breach response (notifying affected individuals, etc.).
6. **Implement Temporary Protections:** Consider additional safeguards in the interim. For example, if a software you use is compromised, you might block its network access or run it in a restricted environment until it's confirmed safe. If a supplier's login credentials were stolen (like API keys or VPN credentials), disable those keys or change those passwords immediately.
7. **Document and Proceed to Containment/Eradication:** Much of the immediate response to a supply chain incident overlaps with **containment strategies** – isolating systems, disabling compromised accounts, and so on. Make sure to log what actions you took and when. Coordinate further analysis with your IT support and the vendor's security team. Once the immediate threat is contained, move into recovery steps (such as restoring any affected systems or data, covered in a later section).

Every scenario above should be followed by a quick debrief among the response team (even if that "team" is just a couple of people in a small company) to confirm the situation is stabilized. Once immediate actions are taken, the focus shifts to **containment**, detailed next.

Containment Strategies (Stopping the Spread and Limiting Damage)

Containment is about **isolating the threat** so it cannot do additional harm. In a small PHCP/PVF business with limited IT staff, containment steps should be straightforward and executable by whoever manages IT (be it an external consultant or a tech-savvy employee). Key containment strategies include:

- **Isolate Affected Systems:** Physically or logically disconnect any compromised computer, server, or device from the network as soon as possible. For example, if one PC is infected with ransomware or malware, unplug its network cable/Wi-Fi – this prevents the malware from spreading to file shares or other PCs. If an entire segment of the network is affected (say multiple PCs showing symptoms), you might disconnect that segment or shut down the office internet temporarily. **Speed is critical:** the quicker you isolate, the more damage you prevent.
- **Disable Compromised Accounts:** If the incident involves stolen user credentials or an email account takeover, promptly **disable or reset those accounts**. For instance, if a user's email was hacked or a high-privilege account is suspected in a breach, suspend that account's access until it can be secured. Force password resets on any accounts that might have been compromised (including company email, VPN, or cloud service accounts). This stops an attacker from using valid credentials to roam further into your systems.
- **Quarantine Malware:** Ensure your antivirus/anti-malware software runs on infected machines to identify and quarantine malicious files. Many antivirus tools will automatically isolate (quarantine) suspicious files; if one sounded an alert, follow its prompts to contain or remove the threat. If you have centralized endpoint security management, an admin can isolate a machine remotely. If not, manual isolation (unplugging as above) and then running a full scan in safe mode or offline is effective.
- **Network Containment Measures:** Depending on the attack, you might need to **block certain network traffic**. For example, if you detect a particular malware trying to communicate with an external server, your IT support can add a firewall rule to block that IP or domain. In some cases, you may temporarily shut down specific services (like an email server or a website) if they are being actively exploited, until you can patch them. Coordinate these actions with your IT provider; they can often make firewall or router changes quickly even offsite.
- **Preserve System Images/Logs:** As part of containment, try to preserve a snapshot of what happened for later analysis. If you have the capability, take a system image or backup of an affected system before wiping it. Similarly, save log files from servers, firewalls, or any system showing signs of attack. This evidence is invaluable for determining root cause and verifying that the threat is fully eradicated. In practice, your external IT specialists or an incident response firm can handle imaging and log collection if you involve them early.

- **Coordinate with Third Parties:** If a third-party service or partner is involved (such as an MSP or a cloud provider), work together on containment. They might take actions like disabling your account or service on their end to stop further damage. Ensure there's clear communication: for instance, if your cloud storage was breached, ask the provider to temporarily lock down all access or rotate API keys. Two-way communication ensures both you and the partner are containing the incident from both sides.
- **Short-Term Fixes:** Apply any immediate fixes available. If the attack vector is known (say a vulnerability in software), apply the patch **immediately** on all systems to prevent the attacker from using it elsewhere. If the incident is a virus outbreak via USB drives, consider temporarily banning all USB usage. These are interim controls to plug the hole that the attacker came through.

The guiding principle of containment is **"stop the bleeding"**. Whether it's unplugging a machine, disabling a user account, or blocking an IP range, do what is necessary to prevent the situation from getting worse. It's acceptable if some operations are halted during this time – it's better to temporarily lose a service or segment of your network than to let an infection or attacker spread unchecked. Once containment is achieved (the threat is no longer active or spreading), the team can move on to notification and recovery efforts.

Reporting Procedures (Who to Notify and When)

Timely and transparent reporting is a critical part of incident response. Even a small company must ensure the right people know about the incident so that proper support and legal steps can be taken. Reporting can be divided into **internal notifications** within the company and **external notifications** to outside parties. Here's a high-level guide on both:

- **Internal Reporting:** Establish an internal communications plan for cyber incidents. Immediately inform the **key decision-makers** in your organization about the incident. In a PHCP/PVF company, this might be the owner, general manager, or a designated incident lead. If you have any IT personnel or an external IT service, they should be looped in without delay (likely they are already aware if they helped contain the issue). Provide a brief factual summary of what's known: e.g., "Our order processing computer was

hit by ransomware at 8:00 AM" or "We suspect an employee email account was compromised." The goal is to ensure management is aware of the situation's severity. For significant incidents, also notify your board of directors or investors as applicable – no one likes surprises when operations are impacted or customer data is at risk. Internally, it's wise to assign a point person (or small team) to manage the incident and communication. All staff should know **who** to contact if they notice something (this should be pre-defined; e.g., "Report immediately to the Operations Manager and call the IT support hotline"). As the incident unfolds, keep employees informed in a controlled manner. Let them know if they need to take action (like "do not use the file server until further notice" or "change your email password today as a precaution"). Keeping staff in the loop can also quell rumors – they'll be less panicked if they hear official updates. However, share information appropriate to their role – for example, if customer data is breached, employees should be told to be prepared for customer inquiries, but sensitive details should be restricted to those handling the response.

- **External Reporting:** You may have legal and ethical obligations to report certain incidents to parties outside your company. Key external notifications include:
    - **Law Enforcement:** Always remember that a cyber attack is a crime. Report serious incidents to law enforcement promptly. For instance, if ransomware has impacted your business or you've suffered a major data theft, you should contact authorities. In the U.S., this typically means notifying your local FBI field office or using the FBI's Internet Crime Complaint Center (IC3) to file a report. Law enforcement can provide guidance and may investigate, especially if it's part of a larger attack campaign. Even if you're embarrassed, reporting is important – many cyber incidents go unreported, but the more people report, the better chance authorities have to identify and catch the perpetrators. (If the incident involves things like credit card theft, you may also need to notify local police or Secret Service; your legal counsel can advise.)
    - **Regulators and Compliance Bodies:** Depending on your industry and the nature of the breach, you might be **legally required** to report to certain regulators. For example, if personal consumer data is compromised, state data breach laws could require you to notify state authorities or the affected individuals within a certain timeframe. If any of your business falls under HIPAA (health-related info) or

other regulations, you'd have specific reporting rules. In the PHCP/PVF sector, regulatory reporting is less common unless you keep personal data (like a large customer loyalty list or employee personal info). Nonetheless, check if any regulations apply. In the UK, for instance, companies report personal data breaches to the Information Commissioner's Office (ICO). In the US, there isn't a single regulator for all breaches, but state Attorneys General often require notification for breaches of personal info. Also, if you're part of an industry association or certification (for example, a partner program that requires reporting incidents), ensure you comply with those. When in doubt, consult legal counsel on your obligations.

- **Affected Customers/Partners:** If the incident impacts customers, suppliers, or partners, you need to inform them in a timely and appropriate manner. "Impacted" means their data was compromised or they will feel the incident's effects (like your systems being down). For example, if customer order information was stolen or will be delayed due to an attack, you should notify those customers. Likewise, if a supplier's info was involved, let them know. When notifying external parties, **be honest and concise** about what happened and what you're doing. Provide guidance if they need to take action (such as "reset your password" or "monitor your credit card for fraud" if applicable). Avoid technical jargon; use plain language to explain the situation. Also, choose the appropriate channel – some notifications might be done one-on-one (a phone call to a major client) versus a mass email or public notice for a broader group. Keeping external stakeholders informed maintains trust and can prevent bigger fallout. Many customers prefer to hear bad news directly rather than through rumors or media.
- **Cyber Insurance Provider:** If your company has cyber insurance, **notify your insurance carrier immediately** after an incident. Most cyber insurance policies require prompt notification of any events that could lead to a claim. The insurer may provide resources like an incident response team, legal counsel, or negotiators for ransomware. They can also guide you on next steps to ensure you don't inadvertently invalidate coverage. For example, some policies have specific clauses about not paying ransoms without insurer consent, or using approved vendors for forensic analysis – loop them in early to

align with these requirements. Even if you're unsure whether you'll claim, it's better to put them on notice. They may also advise on communications and help calculate impacts.

- **Industry Information Sharing:** Consider sharing information about the attack with industry groups or threat-sharing programs (ISACs) if available. For instance, the broader supply chain community (manufacturing/distribution) might benefit if you share, "We were hit by X ransomware variant" or "Beware of fake emails pretending to be from [Vendor Name]." In the US, you can also report incidents or anomalies to CISA (Cybersecurity and Infrastructure Security Agency) via their 24/7 reporting portal or email (report@cisa.gov). While this is voluntary, CISA uses these reports to alert others and can offer help or intelligence in return. In short, if you have reliable channels to contribute to the community's awareness, doing so can turn your incident into actionable intelligence for others.
- **Media/Public Relations:** Small companies may not have to worry about press releases, but if an incident becomes public (e.g., customers post about a breach on social media, or operations are halted for days affecting many), you should prepare a public statement. Assign a spokesperson (usually the owner or a PR representative) to handle any media inquiries. Keep the message consistent with what you told customers: acknowledge the issue, stress what you're doing to fix it, and protect customer interests. Don't speculate on unconfirmed details in public. In many cases, a brief press release or website notice suffices for transparency, especially if customer data was involved. **Note:** For an industry-specific context, if a breach or ransomware attack will significantly delay your ability to deliver products (pipes, valves, fittings, etc.), a public update may be wise to manage customer expectations and rumors in the market.

In all reporting, **timeliness and accuracy** are key. Internal reports should happen as soon as an incident is verified (often within minutes or hours of discovery). External notifications, especially to affected individuals or law enforcement, should occur within 24-72 hours depending on the severity and legal requirements (some data breach laws mandate notification within 30 or 60 days – but it's best not to wait that long if people are at risk). Document all notifications: who was informed, when, and what was said. This documentation is useful for compliance and later review.

Finally, consider seeking **legal advice** early in the process for serious incidents. An attorney experienced in cybersecurity can help draft customer communications, guide regulatory reporting, and protect the company's interests (for example, ensuring any admission of breach is carefully worded). If you have cyber insurance, they often cover or recommend breach coaches (lawyers) for this purpose. Engaging legal counsel ensures you meet obligations and handle the incident professionally.

Recovery & Remediation (Restoring Operations Quickly)

After the incident is contained and urgent notifications are made, the focus turns to **recovery** – getting your business back to normal safely. In the PHCP/PVF industry, downtime can disrupt supply deliveries and customer needs, so a goal of this plan is to restore critical operations **as soon as possible (ASAP)**, ideally within the same day for minor incidents or a few days for major ones. Recovery goes hand-in-hand with remediation, which means fixing the root cause and cleaning up any lingering threats. Key steps include:

- **Evaluate Damage and Priorities:** First, assess what systems or data were affected and prioritize what needs to be restored **first**. For instance, if your order processing system was taken down by ransomware, that's a high priority to restore (because it directly impacts sales and customers). If a less critical system (like an internal HR file server) was hit, that might be secondary. Make a list: what must be up ASAP (for business continuity) and what can wait a bit longer. This will guide your recovery order.
- **Restore from Backups (When Available):** The fastest way to recover from ransomware or data corruption is often to **restore clean backups** of your systems and data. If you have recent backups of the affected servers or files, start the restoration process as soon as containment is done. For example, if a file share was encrypted, you would wipe that server clean and then restore the files from the latest backup copy. Make sure to scan restored data with antivirus before putting it back in service, just in case the backup itself captured some malware (though if backups were offline and from before the attack, they should be clean). If you don't have full system backups, you might have export of critical data (like an Excel of customers or an ERP database dump) – import that into a fresh system build. **Note:** Always verify the integrity of backups regularly

before an incident occurs; nothing is worse than finding out your backups failed when you need them most. Testing backups is a preventative task that pays off hugely during recovery

- **Rebuild or Repair Systems:** For systems without backups or those compromised by malware, you'll need to **clean and rebuild**. This could mean re-installing operating systems or software on wiped machines to ensure they're malware-free. It's often faster and safer to re-image an infected computer than to try to surgically remove a deeply entrenched virus. If hardware was damaged (less common, but possible if an attacker sabotaged devices or if a hard drive failed), replace the hardware and then restore data. Standard steps include reinstalling the OS, applying all updates/patches, reinstalling applications, and then restoring data from backup. While rebuilding, also close any holes: for example, if the breach happened due to an outdated server, make sure the new server is fully patched and perhaps add extra security (firewall rules, etc.) before putting it online.
- **Eradicate Any Remaining Threats:** Ensure that the cause of the incident is fully addressed so it doesn't recur immediately. This might involve:
    - **Patching Vulnerabilities:** Apply all security patches to systems to fix bugs that were exploited. For instance, if the attackers got in through an unpatched Windows server vulnerability, patch all your Windows servers/workstations now.
    - **Improving Authentication:** If the incident was due to a weak or stolen password, reset passwords (preferably require strong ones) and implement multi-factor authentication to make accounts more secure. This includes not just the one compromised account, but any account that could be at risk. It's wise after a breach to enforce company-wide password changes, especially for privileged accounts.
    - **Removing Malware:** Run full anti-malware scans on all systems network-wide to ensure no traces of the virus/backdoor remain. Sometimes attackers leave "persistent" malware (like a hidden remote access tool) to return later – a thorough cleaning is required. Use up-to-date antivirus and possibly specialized anti-rootkit or anti-malware tools recommended by your IT support. In critical cases, a professional incident response team might do a threat-hunt to be sure the environment is clean.
    - **Restoring from Gold Standard:** In some cases, you might rebuild from scratch using known good software images/configurations. For example, wipe

an infected PC and set it up as if new, then restore data. This eradicates any deeply hidden compromises that scans might miss.

- **Recover Operations Step-by-Step:** Bring systems back online one at a time, verifying each is functioning normally. For example, after restoring a database, test that your front-end application can connect to it. After cleaning PCs, have users log in and confirm they can access what they need. Monitor the network for any strange behavior as you reintroduce systems. It's wise to keep everything in a "heightened alert" state for a few days – meaning IT watches closely for any sign of the attackers still in the environment.
- **Communicate Recovery Progress:** Internally, let staff know what services are back up and which remain under maintenance. If customers were aware of the outage, send a follow-up once key services are restored (e.g., "Our ordering system is back online as of 5 PM today. We are working through backlogs but operations are returning to normal."). This reassures stakeholders and provides transparency. It's also good PR to inform customers that you've resolved the issue, especially if their data or orders were affected.
- **Post-Incident Cleanup:** Beyond the immediate fix, carry out any additional remediation needed. This could include:
    - **Changing all system and database passwords** (just in case they were compromised, do this especially if it was a serious breach or ransomware event).
    - **Reissuing employee credentials or ID badges** if an insider or physical breach was involved.
    - **Restoring lost data manually** if something was not backed up (for example, re-entering paper records that were only on the system that got wiped).
    - **Monitoring Credit or Identity Theft Protection** – if customer personal data was stolen, you might consider providing an identity theft protection service for those customers for some period, as remediation (and goodwill).
    - **Policy or Configuration Changes** – fix any security policy gaps identified. For example, if the breach happened because a firewall port was left open, close it and update your firewall rules documentation.
- **Validate the Fixes:** Once everything is up and running, do a mini "audit" of the incident's root cause to ensure it's truly resolved. If the incident was ransomware, make sure restored systems are truly ransomware-free and confirm that the vulnerability that allowed it (like RDP remote access with no MFA) is addressed. If it was a phishing-born malware, ensure the specific malware is eradicated and

perhaps run a penetration test or vulnerability scan after recovery to double-check your environment's security. Essentially, **test that your systems are secure and normal operations have resumed**.

- **Record Lessons and Update Documentation:** As part of closing out the recovery, document exactly what was done to recover. Note how long each step took, any challenges faced, and what could be improved. This will feed into the "lessons learned" process. Additionally, update your inventory and network diagrams if systems changed (for instance, if you deployed a new server or changed configurations as part of remediation, make sure your records reflect that). Having accurate documentation will help in any future incidents or audits.

Throughout recovery, keep in mind the objective: **restore critical business functions as fast as possible, but safely.** "Safely" means you don't want to rush to bring things back only to be hit again by the same threat. It's a balance – speed is important, but thoroughness in cleaning up will save pain later. If you have the option, you can perform recovery steps in parallel: e.g., while IT is rebuilding a server, management can work on customer communications or temporary workarounds to keep business running.

If certain operations cannot be restored same-day (say a particular system will take time), invoke your business continuity plans. For example, maybe you temporarily switch to manual processing of orders (taking notes on paper or spreadsheets) while the system is down. The incident response plan should interface with your broader **business continuity/disaster recovery plans** here – those plans detail how to operate manually or in degraded mode until full recovery. Strive to implement stopgaps so the business can function at some level during the remediation period.

Lastly, once recovery is complete, consider a formal **post-incident review** (described in Framework Flexibility below). This will cement the improvements and ensure any remaining issues are addressed.

Prevention Measures (Cyber Hygiene)

"An ounce of prevention is worth a pound of cure." While this plan focuses on incident response, the best outcome is avoiding

incidents in the first place. For PHCP/PVF companies, cybersecurity can feel daunting, but a handful of **simple, high-impact practices** go a long way. Implementing these does not require deep expertise – just consistent attention and possibly some outside help for setup. Here are practical preventative measures tailored for low IT maturity environments:

- **Regular Data Backups (with Offline Copies):** Ensure you back up important business data frequently and keep copies **offline or offsite** (not just connected to your main network). For example, back up your accounting system, customer database, and key documents to an external USB drive or a cloud backup service. **Unplug or secure the backups** so ransomware or an attacker cannot reach and encrypt them. Test your backups periodically by restoring a file to confirm they work. Reliable backups are your fastest recovery tool and the best defense against ransomware – if you can restore data, you don't need to pay ransom.
- **Keep Systems and Software Updated:** Outdated software is a common entry point for attackers. Enable automatic updates on your computers, servers, and devices whenever possible. This includes your operating systems (Windows, etc.), web browsers, Office software, and any specialized industry software (like inventory or building controls). Also keep network devices (routers, NAS drives, etc.) updated by applying firmware patches. Many attacks succeed simply because a known vulnerability wasn't patched. Make someone responsible for weekly checking that updates succeeded. If a system can't be auto-updated, schedule a regular manual update or get IT support to handle it. In short, **don't ignore those update prompts** – they often fix critical security holes.
- **Use Strong Passwords and Multi-Factor Authentication (MFA):** Require that all user accounts use strong, unique passwords (preferably passphrases) and whenever possible, enable MFA for an extra layer of security. MFA (such as a one-time code on a phone or a hardware token) is **one of the most effective measures** to prevent unauthorized access. At a minimum, ensure that email accounts and any remote access/VPN accounts have MFA turned on, since those are prime targets. Many cloud services (Office 365, G Suite, etc.) offer MFA – take advantage of it. Also, never share passwords between employees, and avoid using default passwords on equipment. Consider a password manager for the company to help users manage complex passwords easily.
- **Security Awareness Training for Staff:** Humans are often the weakest link, but they can become a strong defense with basic training. Educate employees about common

cyber threats like phishing, suspicious links, and social engineering. Teach them not to click unknown email links or open unexpected attachments, and to be cautious with emails or messages that create a sense of urgency or ask for sensitive info. Regularly remind and update staff on new scam techniques (phishers constantly evolve their tactics). Even a short annual training session or circulating examples of real phishing emails can significantly reduce risky behavior. Emphasize that no one will be punished for reporting a potential security incident – in fact, it's encouraged. Consider leveraging free resources or small business cybersecurity kits that provide tip sheets for employees. Building a security-aware culture is cost-effective and vital.

- **Secure Email and Internet Use:** Since email is the top delivery method for malware and fraud, implement protective measures on your email system. Use spam and phishing filters to automatically block or quarantine suspicious messages (most email providers or Microsoft 365/Google Workspace have these features built-in). Enable **email authentication protocols** like SPF, DKIM, and DMARC to prevent spoofed emails appearing as your domain– your IT provider can help set this up. Additionally, install a reputable antivirus/internet security suite on all computers and keep it updated. This software can block malicious websites and detect malware before it runs. Encourage safe browsing habits: don't allow random software downloads, and restrict administrator privileges (users should not be browsing the web or checking email while logged in as an admin). If employees use USB drives, consider scanning them or restricting auto-run features to avoid infections.
- **Firewall and Network Security:** Use a firewall on your internet connection to filter traffic. A basic business-class router/firewall can prevent many external attacks by closing unnecessary ports. Make sure remote access to your network (like Remote Desktop or VPN) is secured with strong passwords and MFA, or disabled if not used. Change default passwords on all network devices (routers, Wi-Fi, cameras, etc.). Segregate networks if possible – for example, have a guest Wi-Fi separate from your main business network, so an infected guest device can't reach your company machines. For companies with warehouses or building control systems, isolate those operational networks from the corporate network as much as feasible; this limits the spread if one gets compromised.
- **Principle of Least Privilege:** Give employees the minimum access privileges they need to do their job, no more. For instance, not everyone should have admin rights to company PCs or access to all shared drives. By limiting

access, you reduce the damage if one account is compromised or if an insider decides to snoop. Review user access rights periodically – when someone changes roles or leaves the company, update or revoke their access promptly (have a checklist for employee off-boarding to remove accounts, etc.).

- **Secure Physical Devices:** Cybersecurity isn't just digital – ensure your physical environment is secure too. Keep servers or networking gear in locked rooms or cabinets to prevent tampering. Use cable locks or other security for laptops if stored in less secure areas. Ensure that if an employee leaves, they return company devices and their accounts are disabled immediately (to prevent any disgruntled actions). Also, encourage using device encryption (built-in on modern OS like BitLocker for Windows or FileVault for Mac) for laptops, so if one is stolen, the data isn't easily accessible.
- **Plan for Outsourced IT Support:** Since PHCP/PVF firms may not have full-time IT staff, establish a relationship with a reputable **managed service provider (MSP)** or IT consultant. They can handle many of the above preventative measures (patch management, monitoring, backups) on your behalf. Do due diligence – ensure they have good security practices themselves. As part of your contract, set clear expectations that they will help in incident response promptly. An external partner can also maintain your incident response plan's technical aspects, like ensuring the phone tree is up to date or that they have remote access set for emergencies. Essentially, don't wait for a crisis to find IT help; have them on standby. Many small businesses opt for a retainer or service agreement so that when something goes wrong, the experts are just a call away. This is like having an "IT fire department" – you hope to never need them for a fire, but you're glad they're there.
- **Cyber Insurance and Response Planning:** As part of risk prevention, consider purchasing cyber insurance (if you haven't already). It can provide financial protection and access to incident response experts in case of a major cyber event. Make sure you understand the policy – know what's covered and any requirements (such as maintaining certain security measures). Cyber insurance often comes with or subsidizes pre-breach services like security training or risk assessments which can further reduce your chances of an incident. It's not a substitute for good security, but an additional safety net.
- **Continuous Improvement:** Cyber threats evolve, so your defenses should too. Keep informed of major threats targeting businesses like yours. A good practice is to sign up for alerts from credible sources like CISA or an industry

association. They often send advisories (e.g., "urgent patch for Windows" or "new phishing scam going around targeting distributors"). With minimal effort, you can stay ahead of emerging risks. Also, periodically evaluate your security practices – perhaps annually, go through a checklist (there are "Cybersecurity Essentials" checklists for small businesses available) and see if there are new simple things to add or old things to improve. Cybersecurity is an ongoing process, not a one-time project. Implementing the above measures creates layers of defense: even if one fails (say someone clicks a bad link), another (up-to-date antivirus or MFA) will stop the threat, or at least your backup will save the day. These hygiene steps significantly lower the likelihood of incidents – and when incidents do happen, they reduce the impact (for example, strong network segmentation might confine a ransomware to one PC instead of the whole company). **For a small investment of time and resources, these practices pay off by protecting your business's continuity and reputation.**

Framework Flexibility and Maintenance of the Plan

No two companies or incidents are exactly alike. This response plan is a general framework, and each PHCP/PVF company should **tailor it to their specific circumstances.** Flexibility means you adapt the plan to your size, your team's skills, and the technology you use, and you keep the plan updated as things change. Here's how to ensure the plan remains effective and customized:

- **Assign Roles and Responsibilities:** Even a small company should designate who is responsible for what during an incident. Tailor the plan by naming those people or roles in your company. For example, decide in advance who will coordinate with external IT support, who will handle communications to customers, and who has authority to shut down systems if needed. Document these in the plan (e.g., "Office Manager: coordinate internal incident communications; Warehouse Supervisor: ensure backups are accessible and verify inventory system recovery," etc.). If you have an IT provider, include contact names and emergency numbers for them in the plan. Clarity on roles prevents confusion during a crisis. Also prepare a **contact list** (phone and alternate email) for all key persons and

keep a hard copy accessible; during a severe incident you might not have access to your digital contacts.

- **Customize to Infrastructure:** Update the plan to reflect your actual IT environment and business operations. For instance, if you don't have a certain system (maybe you use only cloud services and have no physical servers), adjust the recovery section for that – focus on cloud account recovery rather than server restores. If you have specific equipment like inventory management tools, add notes on how to handle those (perhaps power-off procedures or vendor support contacts). Essentially, make the plan *yours* – the more it references your actual network drives, applications, and vendor contacts, the more actionable it will be during an incident.
- **Practice the Plan:** A plan on paper is good; a practiced plan is **far better**. Conduct periodic drills or tabletop exercises to walk through incident scenarios**.** For example, gather the team and say "It's a Tuesday morning, and our main order processing system just got hit with ransomware – go!" Then discuss, step by step, how each person would respond according to the plan. This helps reveal gaps or confusion in a low-pressure setting. Tabletop exercises can be done quarterly or at least yearly, and they greatly improve readiness. Even a short role-play where an employee "reports" a fake phishing email and the team talks through the response can highlight if everyone knows their role. After drills (or real incidents), debrief to see what worked and what didn't, and **update the plan accordingly**.
- **Keep the Plan Updated:** Treat this incident response plan as a living document. Regularly review and revise it to account for changes in your business or the threat landscape. At a minimum, review it annually. If you add or remove IT systems, change service providers, or have key staff turnover, update the plan immediately to reflect new realities (e.g., "New backup solution X is now in use – here's how to restore from it"). Also, incorporate lessons learned from any security "near misses" or actual incidents – if an incident revealed that communication was slow, you might update the internal call tree or procedures. **Cyber threats are always evolving, so your plan should evolve too**. Regular reviews will keep it effective.
- **Integrate with Business Continuity/Disaster Plans:** Ensure your cyber incident plan meshes with any overall business continuity plan. For instance, if you have a general disaster plan for fires or natural disasters, align the recovery strategies (both plans might rely on the same backups or alternate work locations). This avoids conflict and ensures that recovering from a cyber incident doesn't overlook other business continuity needs.

- **Framework vs. Specifics:** The plan provides a general framework but allows flexibility in execution. That means during a real incident, staff should feel empowered to make reasonable adjustments on the fly if needed. For example, if the plan says to contact a particular manager who happens to be on vacation, the team should know to contact the backup person or another executive instead. Emphasize **guiding principles** (like "stop spread, protect safety, communicate clearly") so that even if specifics differ, the response aligns with the plan's intent. Encourage a mindset of **"use the plan, don't be a slave to it."** It's there to guide, not to cover every imaginable detail. As long as actions taken follow the spirit of the plan and are documented, the plan is working.
- **Management Support and Formalization:** Have leadership formally approve and support the incident response plan. This gives it weight in the organization – everyone knows this is the official procedure. Leadership support also means you're more likely to get resources for training or preventive measures. Present the plan to all employees (perhaps in a meeting) so they know it exists and understand the basics. Keep a copy of the plan accessible (both electronically and a hard copy in case your network is down during an incident).
- **Leverage External Guidance:** Stay adaptable by leveraging external cybersecurity frameworks or guidelines. For instance, the **NIST incident response lifecycle** (Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned) underpins much of this plan, and you can use NIST or CISA resources for more detail on any phase. The plan can be mapped to such frameworks if needed, which makes it easier to adjust when new best practices emerge. Also, maintain contacts with external experts (as noted, IT consultants, cyber insurance, etc.) – they can provide template updates or advice as threats change.
- **Continuous Learning:** After each incident (even minor ones), do a "post-mortem" analysis: What happened? Why? How well did the response go? What could we do better or faster? Document these lessons. This should directly inform updates to both your security measures (prevention) and the response plan. Many organizations find that every incident (or near miss) uncovers something to improve – maybe it's as simple as "we need to have a printed phone list at home for after-hours incidents" or "next time, we'll call our IT provider sooner." Over time, these iterative improvements make the plan more bulletproof and the team more confident. In essence, **learn from the incident** and refine your strategies. By keeping the plan flexible and up-to-date, a small company can punch above its weight in

cybersecurity readiness. The document you create today shouldn't sit on a shelf; it should evolve with your business. Cyber threats may be continuously changing, but a well-maintained and practiced plan ensures your response will be swift and effective no matter what comes your way. Remember, the goal of this plan is to minimize damage and downtime – by adapting it to fit your environment and revisiting it regularly, you ensure it will do exactly that when an incident strikes.

References:

- NCSC – *Small Business Guide: Response & Recovery* – Practical steps for identifying incidents and resolving them.

  westtek.co.uk

- CISA (US) – *Cyber Guidance for Small Businesses* – Emphasizes executive support, staff training, and maintaining an incident response plan (IRP) with regular reviews.

  cisa.gov

- CISA – *Ransomware Response Checklist* – Recommends immediate isolation of infected systems and consulting law enforcement for decryptors.

  cisa.gov

- FTC (US) – *Cybersecurity for Small Business* series – Offers plain-language steps:
  - **Ransomware:** Plan ahead, backup data offline, keep software updated, train staff, disconnect infected systems, and involve the FBI if attacked.

    ftc.gov

    Phishing: Educate employees, use email authentication, if compromised change passwords, disconnect devices, follow internal procedures, notify affected customers, and report scams to authorities.

    ftc.gov

ASA / Supply Industry resource – Contextualizes the PHCP/PVF industry (plumbing, heating, cooling, piping and industrial pipe, valves, fittings) and its business continuity importance.

supplyindustrycareers.com

Highlights that even non-IT-intensive sectors play a critical role in daily life, hence the need for cyber resilience.

- SentinelOne – *Insider Threat Guide for Small Businesses* – Notes that 31% of data breaches in 2023 were caused by insiders, underlining the importance of monitoring and controlling internal risks.

  sentinelone.com

- Mid Penn Bank – *Creating a Cyber Incident Response Plan for Small Business* – Reinforces including procedures for various attack types (ransomware, data breach, phishing) and establishing communication protocols for internal/external stakeholders

  midpennbank.com

- NIST SP 800-61 – *Computer Security Incident Handling Guide* – Incident lifecycle framework (Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned) that informs best practices in this plan.

  westtek.co.uk

  (NIST guidance stresses learning from incidents and adjusting plans accordingly.)

- CISA – *Insider Threat Mitigation Guide* – Advises reporting illegal insider activities to appropriate authorities and developing a holistic program to address insider risks.

  cisa.gov

- Redscan/Kroll – *Incident Response for Small Businesses* – Highlights the value of an incident response retainer and assigning clear responsibilities and escalation paths in a small business IR plan.

  redscan.com