Planning and preparing for the next incident

Preparation

1. Create and review incident response policies as well as conducting a thorough risk analysis of your environment.
2. Train! Simulate incidents and test response activities. Confirm compliance with policies;
3. Post policies in key departments.
4. Engage third parties to review and update policies to ensure best-practice responses; and
5. As a starting point, see our Data Security and Best Practices Guide at: Exhibit C

Detection

6. The timing of detection is critical. You typically have 48 hours or less to recover funds.

Response

7. Containment is critical once the event is discovered and further damage must be mitigated.
8. No changes should be made on the device or devices impacted without security/IT approval.
9. An image of the system(s) should be executed and stored for forensic investigators.

Mitigate

10. Build an understanding of what was compromised on the system, so the system can be properly recovered.
11. The method of recovery will be dependent on this phase and remediation steps will begin here.

Report

12. This should not be confused with the above-mentioned reporting of the “Financial Fraud Kill Chain”. This is information that should be collected and used for informing key stakeholders as well as future training to demonstrate the incident as part of the preparation phase noted above.

Recover

13. In connection with the mitigation efforts, remediation could be a simple email password change or as involved as rebuilding the machine. At this point, the system is restored to its former operational status.

Post Mortem

14. Obtain and document a comprehensive summary of the events that lead to the breach or loss.
15. New risk mitigation controls should be implemented to prevent further incidents - once we know better, we should do better.

CertifID is a guaranteed solution that prevents fraud and restores trust in transactions. Harnessing and analyzing billions of combined personal, and digital records, a “digital truth” is established that confirms you are exchanging information with the person you intend to. This allows you to act with confidence and focus on the customer experience rather than worrying about fraud.

For more information, or to start a conversation,
please visit www.citadelcybersolutions.com and www.certifid.com.

Exhibit C

Data security encompasses a wide variety of practices, methods, and procedures based on the type of organization, technology topology (on-premises, cloud, or hybrid) and type of data being protected. While not all of these combinations can be accounted for in a single document, there are general concepts that can help direct the planning process for any organization. These practices can be divided in terms of Systems, People, and Processes which can address the confidentiality, integrity and availability of systems and data.

All the practices below should be put into the context of standards. The most popular standards in the market place today can help guide you through the implementation of your security program and ensure the right security posture for your organization. While not comprehensive, below are some of the most popular standards in use today:

- ISO/IEC 27001 - Information security management systems
- NIST Cyber Security Framework
- NIST Small Business Security (The Fundamentals)
- Center for Internet Security – Best Practices
- ISACA - Control Objectives for Information and Related Technologies (COBIT)
- Open Web Application Security Project (OWASP)
- Information Technology Infrastructure Library (ITIL)

While the list below is not exhaustive its purpose is to show the base building blocks of controls that should be in place to ensure a sound and secure environment. For expanded views into other controls, review the ISO 27002 and NIST 800-53 control documents which go into much greater detail and explanation.

Systems

Perimeter

Appliances such as firewalls, routers, and specialized equipment for Intrusion Detection, Log Monitoring and Artificial Intelligence (AI) can all play a role in hardening an environment such as:

- Web content filtering
- Anti-virus scanning
- Reputation, application, and protocol protection
- Advanced threat protection for zero-day exploits
- Data loss prevention and auditing policies
- Deep Packet Inspection of HTTPS traffic
- Geolocation-based blocking
- Intrusion detection

Wireless security

- Identity-based 802.1x authentication
- Wireless intrusion prevention
- Properly separated guest, employee and production networks
- Mobile device management

Systems monitoring

- Collection of logs at every critical point in the network, including firewall/router and front-end and back-end systems
- Security monitoring and alerting based on smart triggers

Use of AI to spot hard to see intrusion and data exfiltration attempts

Infrastructure

- Redundant, robust, and encrypted backup strategy including cloud and other off-premise backups
- Data classification
- Data encryption at rest and in transit
- Data tokenization
- Email digital signatures
- Email encryption
- Use industry leading spam, malware, and virus filters, to filter and protect against spam, viruses, phishing, and malicious attachments
- Enable two-factor authentication to domain registrar, DNS, and other hosting environments
- Implement DNSSEC to ensure that DNS records cannot be compromised or taken over
- DKIM and SPF record to protect against malicious domain spoofing
- Ensure OS and third party applications are patched according to vendor recommendations

EXHIBIT C

People

Perimeter

- Train employees to be aware of anything that might look different outside of their normal world. This can include email, phone, other forms of communication, or people without proper identification. Train with real examples to make a strong impact. Red team exercises are also beneficial
- Never enter login information outside of the normal outlets, especially email
- Don't open unexpected, unsolicited, or suspicious attachments. Always verify with IT when possible
- Ensure data is saved to trusted network/server locations and do not allow USB storage devices
- Conduct unannounced phishing testing on a periodic basis using a trusted, third party firm
- Conduct and track regular training of employees using a trusted, third party firm
- Prevent "Shadow IT" cloud services by auditing access logs, financial records, and user behavior
- Ensure all users have access to and have read and acknowledge security policy documents

Physical

- Locked doors with proper access to employee and infrastructure areas
- Clean desk policies
- Proper identification for staff and vendors
- Security cameras

EXHIBIT C

Processes

Access controls

- Role-based file permissions
- File system and application specific permissions
- Dedicated service accounts to isolate access to critical systems if one is compromised
- Least privileged accounts with minimum required access
- Complex, yet enforceable, user password policies
- Multi-factor authentication
- VPN connections for remote users
- Penetration testing utilizing services

Client and endpoint security

- Software restriction policies
- Removing administrator permissions from users
- Regular antivirus scans and reporting

Infrastructure

- Disaster recovery and incident response planning
- Emergency preparedness for natural and manmade events

Audits

- Conduct scheduled internal audits of your security program to determine any actions that need to be taken to remediate the program. A plan that includes the: DO, CHECK, and ACT process can help you continuously monitor and improve your security stance
- Conduct annual external audits led by third parties to ensure compliance with best practices and current standards
- Conduct third party risk assessments on all vendors annually or more frequently as the business process requires

CERTIFID

1410 PLAINFIELD AVE. NE, GRAND RAPIDS, MI 49505
PHONE NUMBER: (616) 855-0855
WWW.CERTIFID.COM
SUPPORT@CERTIFID.COM

CERTIFID

1410 PLAINFIELD AVE. NE, GRAND RAPIDS, MI 49505
PHONE NUMBER: (616) 855-0855
WWW.CERTIFID.COM
SUPPORT@CERTIFID.COM