Grant Thornton

COVID-19 and Cybersecurity

Respond and restore. Together.

Protecting value during a global pandemic

As the global COVID-19 pandemic fundamentally changes the way we live and do business, it is crucial that your organization's security posture remains a priority.

Hackers and adversaries thrive on periods of uncertainty and crisis. Historically, cyber criminals take full advantage of the chaos brought on by floods, fires, wars, and other chaotic events in order to commit fraud, theft, or other nefarious activities. The unprecedented global impact of COVID-19 on all aspects of our health, way of life, and economy present some unique risks and realities that should be carefully accounted for within your organization:

- Video conferencing & collaboration tools
- Social engineering & security awareness
- Incident response & contingency operations
- Physical & logical access limitations
- Reduced workforce & separation of duties

COVID-19 Challenge

Video conferencing & collaboration tools

Expansion of remote access and work from home orders introduce inherent risks in terms of user activity, unauthorized software, and unsecured wireless access points.

Social distancing has significantly increased the use of free video conferencing and collaboration tools which may not enforce appropriate IT security and privacy safeguards.

Best Practice Solutions

Secure work from home networks

- Ensure staff use secured wireless access points protected at the end user and administrative level. Utilize VPN access to sensitive data and applications whenever possible
- Restrict end user privileges to block downloads of unauthorized software and executables
- Conduct business-related video conferencing and collaboration via trusted, enterprise-level applications in which access and meeting invitations are carefully provisioned

Social engineering & security awareness

During times of crisis, adversaries will focus their efforts on the weakest link in the security infrastructure – typically the human element.

With an ever changing environment of government restrictions, disinformation campaigns, and a multi-trillion dollar stimulus package, the threat of social engineering is at a peak.

Exploitation attempts can take the form of spoof emails (phishing), voice communication (vishing), text messaging (smishing) and/or USB drops.

Double down on security awareness & communication

- Consider weekly security bulletins that include best practice tips, enhanced organizational policies, and incident response procedures to spread awareness
- Utilize threat intelligence feeds from federal, state & local resources, as well as deep web and dark web monitoring for malicious disinformation or exploits
- Leverage technical means to alert users of malicious links, evaluate email attachments from untrusted sources, and block access to known malicious sites

COVID-19 Challenge

Incident response & contingency operations

The "new normal" of COVID 19 has not only impacted your local office, but has forced organizations to reimagine their business processes with intercompany organizations as well as their upstream and downstream supply chain, vendors, and subcontractors.

Those organizations that invested in disaster recovery, continuity of operations, and business impact analysis will certainly be seeing the benefits.

Physical & logical access limitations

Expansion of remote access and work from home orders introduce inherent risks in terms of user activity, unauthorized software, and unsecured wireless access points.

Social distancing has significantly increased the use of free video conferencing and collaboration tools which may not enforce appropriate IT security and privacy safeguards.

Reduced workforce & separation of duties

With many personnel either unexpectedly unavailable due to pandemic complications or workforce modifications, it is possible that accomplishing some critical tasks requiring separation of duties may require temporary assignment re-assignment of personnel or acceptance of risk.

Many CIO/CISOs have lean organizations even in normal operating conditions. When an organization cannot reasonably accomplish a task with a separation of duty control in place, any modification decisions should be deliberately documented and tracked at the appropriate level to minimize future audit concerns.

Best Practice Solutions

Crisis = Opportunity

- Don't let the pandemic crisis go to waste as it presents a significant opportunity to flex your contingency planning an incident response programs.
- Throughout the lockdown, conduct weekly reviews of applicable plans/policies to analyze and document what is working well and what needs to be fixed while in an active DRP/COOP scenario
- Report pervasive social engineering campaigns to legal and government bodies (i.e. US CERT, FBI, Information Sharing & Analysis Centers, etc.).

Minimize the attack surface

- Enforce multi-factor authentication (MFA) for remote users accessing critical business systems.
- Implement mandatory VPN use for users connecting through non-corporate network access points.
- Power-down and disable unused connections in offices which are unoccupied in order to decrease total network traffic and remove potential malicious access or pivot points – this includes printers, LAN connections, desktops, IoT devices, etc.

Document, assess risk, and monitor conflicting roles and activities

- Ensure that any changes to administrative personnel are closely tracked and the appropriate actions are taken regarding privileged accounts upon changes to personnel assignments.
- Audits of privileged accounts should be conducted regularly and compared against personnel assignments in order to ensure that there are no unnecessary or maliciously created privileged accounts.
- Increased logging should be used for all privileged or sensitive accounts to ensure that actions can be audited and tracked going forward.

Cyber Professionals are on the front lines in this fight and we stand ready to assist

On March 28th, 2020 the Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) designated cybersecurity professionals as "essential critical infrastructure workers" during the COVID-19 response. This designation places the cybersecurity workforce in the same elevated category as public and community healthcare, law enforcement, public safety, agriculture, energy and other critical industries at the forefront of this global challenge. The 53,000 professionals of Grant Thornton stand ready to assist our clients and our global community in this call to action.

Dave Simprini
Principal, Public Sector
T 703 373 8698
E dave.simprini@us.gt.com

Grant Thornton

Grant Thornton Public Sector helps executives and managers at all levels of government maximize their performance and efficiency in the face of ever tightening budgets and increased demand for services. We give clients creative, cost-effective solutions that enhance their acquisition, financial, human capital, information technology, and performance management. For more information, visit www.gt.com/publicsector.