IMAGEQUEST℠

CYBER RECOMMENDATIONS AND GUIDANCE SHEET

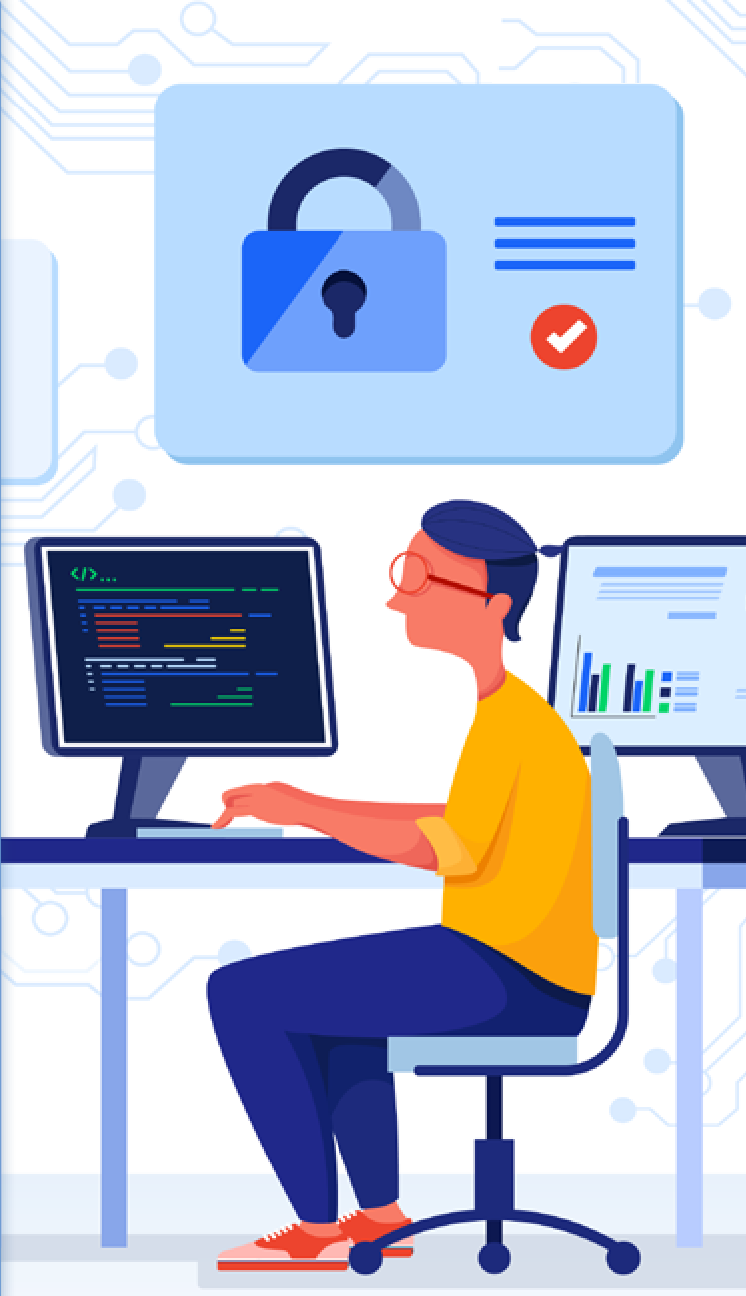
The current geopolitical stress underway in our world means extra vigilance on cybersecurity matters. Cyber is perhaps the easiest and potentially most profitable route to ruining an organization – and by extension, trying to wreck an economy.

If you are a financial institution, a lender, an insurer, a healthcare organization, a manufacturer – or simply a small company providing vendor services to a large target organization – you should assume you are a high-value target to a hacker.

The federal agency responsible for our nation's cybersecurity, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), urges all organizations to take a "Shields Up" stance. Many of the recommendations CISA urges are measures we have been recommending to our clients. We endorse CISA's suggestions and can assist in implementation.

We want to support you and your IT team by providing CISA's recommendations here as a checklist to ensure your organization has the strongest protections in place. Read through this list, and if you or your team have questions or need more information, contact us - or visit CISA.gov.

These recommendations are grouped by actions for executives, actions for IT teams, and actions for individual employees. Some recommendations will be familiar – and some may require additional steps to consider.



A. IT TEAMS

REDUCE THE LIKELIHOOD OF A DAMAGING CYBER INTRUSION

1. Validate that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.
2. Ensure that your software is up to date, prioritizing updates that address known exploited vulnerabilities. CISA has a list here.
3. Confirm that your organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
4. If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong access controls, including attention to email forwarding rules. More information is here.
5. Sign up for some cyber hygiene testing, such as a vulnerability scan or a penetration test. Government agencies and organizations such as utilities can get free cyber hygiene assessments. More information is at the link above. We also offer these services.

TAKE STEPS TO QUICKLY DETECT A POTENTIAL INTRUSION

- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
- Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.
- If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

ENSURE THAT YOUR ORGANIZATION IS PREPARED TO RESPOND IF AN INTRUSION OCCURS

- Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/responsibilities within the organization, including technology, communications, legal and business continuity.
- Assure availability of key personnel; identify means to provide surge support for responding to an incident.
- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

MAXIMIZE YOUR ORGANIZATION'S RESILIENCE TO A DESTRUCTIVE CYBER INCIDENT

- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.
- If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.

CISA also recommends you review its information on specific Russian-sponsored threats – the kinds of malware used and their historical tactics – also on the link above.

B. C-LEVEL EXECUTIVES

- ***Empower Chief Information Security Officers (CISO):*** In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company and ensure that the entire organization understands that security investments are a top priority in the immediate term.
- ***Lower Reporting Thresholds:*** Senior management should establish an expectation that any indications of malicious cyber activity, even if blocked by security controls, should be reported, as noted in the Shields-Up website, to CISA or the FBI. Lowering thresholds will ensure we are able to immediately identify an issue and help protect against further attack or victims.
- ***Participate in a Test of Response Plans:*** Cyber incident response plans should include not only your security and IT teams, but also senior business leadership and Board members. If you've not already done, senior management should participate in a tabletop exercise to ensure familiarity with how your organization will manage a major cyber incident, to not only your company but also companies within your supply chain.
- ***Focus on Continuity:*** Recognizing finite resources, investments in security and resilience should be focused on those systems supporting critical business functions. Senior management should ensure that such systems have been identified and that continuity tests have been conducted to ensure that critical business functions can remain available subsequent to a cyber intrusion.
- ***Plan for the Worst:*** While the U.S. government does not have credible information regarding specific threats to the U.S. homeland, organizations should plan for a worst-case scenario. Senior management should ensure that exigent measures can be taken to protect your organization's most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary.

C. INDIVIDUAL EMPLOYEES

- ***Implement multi-factor authentication on your accounts.*** A password isn't enough to keep you safe online. By implementing a second layer of identification, like a confirmation text message or email, a code from an authentication app, a fingerprint or Face ID, you're giving your bank, email provider, or any other site you're logging into the confidence that it really is you. Multi-factor authentication can make you 99% less likely to get hacked. For the strongest protection, investigate FIDO (Fast IDentity Online) authentication.
- ***Update your software and turn on automatic updates.*** Bad actors will exploit flaws in the system. Update the operating system on your mobile phones, tablets, and laptops. And update your applications – especially the web browsers – on all your devices too. Leverage automatic updates for all devices, applications, and operating systems.
- ***Think before you click.*** More than 90% of successful cyber-attacks start with a phishing email. A phishing scheme is when a link or webpage looks legitimate, but it's a trick designed by bad actors to have you reveal your passwords, social security number, credit card numbers, or other sensitive information. Once they have that information, they can use it on legitimate sites. And they may try to get you to run malicious software, also known as malware. If it's a link you don't recognize, trust your instincts, and think before you click.
- ***Use strong passwords***, and ideally a password manager to generate and store unique passwords. Our world is increasingly digital and increasingly interconnected. So, while we must protect ourselves, it's going to take all of us to really protect the systems we all rely on.

D. CONSULT WITH IMAGEQUEST FOR IMPLEMENTATION

We're sure your IT team has heard of many of these measures but perhaps has not been able to implement them. Or your organization may be completely buttoned up.

Either way now is the time to ensure that you're doing all that you need to be doing!

If your visit to the CISA.gov website leaves you feeling overwhelmed – and worried about what it all will cost – talk with our experts. We can help you and your team comply with the recommendations while freeing up your team to continue working on business initiatives.

If you have questions or want to learn more about ImageQuest's security and compliance services, reach out to us. ***You can start by booking a short confidential consultation here.*** We're standing by to help. Don't delay – world events are moving fast.

Don't risk all you've worked for to a malware attack.