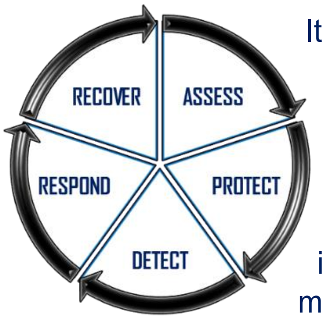
SHIPSHAPE
INFORMATION TECHNOLOGY

Secure Your IT.
Reduce Your Risk.

If 2020 has taught us anything, it is to think beyond immediate realities and to plan for the impact of external forces. These range from politics to pandemics, risky employee behaviors, evolving threats and new technologies.



It also must be understood that IT security is not an event, it is a process. When technology changes, or a pandemic mandates a sea change in how/where we work, cyber criminals innovate and IT professionals work to stay ahead.

By adopting a layered approach to cybersecurity, organizations can increase their vigilance and provide reassurances to client that proper measures have been taken and are being updated.

Within a layered approach, multiple security solutions are deployed to defend different potential attack vectors within your network, preventing a shortfall in any one solution leading to a wider failure.

A Simplified View of IT Security Layers:

PERIMETER	PEOPLE	ENDPOINTS	DATA
The outer edge of your network & the first point of contact for external threats.	*People*, click on links. It's the most common attack vector with the highest success rate for ransomware perpetrators.	Every connected device represents a path to your data, intellectual property & reputation.	Know where it's stored, how it's transmitted, protected, backed up and restored.

Policies & Pandemics

The pandemic is increasingly shifting control to users and away from the security and visibility provided by corporate networks. Policies governing the use of personal systems, where data is stored, how systems are protected and your valuable data is backed up, have never been more critical.

For help developing sound cybersecurity policies, click here to be taken to the National Cybersecurity Society, a non-profit organization focused on providing cybersecurity education, awareness and advocacy to small businesses.

43% of cyberattacks are aimed at small business

$200K The average cost per incident (businesses of all sizes)

14% are prepared to defend themselves

60% of hacked small & medium-sized businesses go out of business after 6 months.

SHIPSHAPE
INFORMATION TECHNOLOGY

Secure Your IT.
Reduce Your Risk.

The following are basic measures that all business must consider.
For assistance with this list, or to answer any questions, contact us by phone:
301.941.1444 Option 2 or email: ITAssessment@ShipshapeIT.com.

- ✓ Centralized and Managed Anti-Virus, Anti-malware, and Operating System updates remove reliance on users to implement updates and provides reporting to track which systems have accepted and implemented and those which are at risk.

- ✓ Avoid 'Bring Your Own Device' (BYOD) for Workstations and Work Phones. Controlling your data and how it is accessed, stored, and backed up is made easier when the device is corporate property. *See note above regarding policies.*

- ✓ Mandate Disk Encryption for mobile and home-based devices. Without it, the hard disk on your laptop can be accessed within a few minutes by cybercrime perpetrators. Windows and Mac systems have this function built-in at no cost. It simply needs to be turned on.

- ✓ Enforce the use of Multi-factor Authentication (MFA). MFA is an authentication method that requires to identify themselves by more than a username and password, decreasing the likelihood of a successful cyber-attack.

- ✓ Implement a formal 'out-of-band' request and confirmation requirement for financial/PHI requests. If an email is received asking for sensitive personal or financial information, have the user call the sending party to verify the validity of the request.

- ✓ Phishing is the number one security threat to your business. Deploying Internet Security Awareness training, (ISAT), which tests users via phishing simulations, is vital in avoiding falling prey to an actual phishing attack.

- ✓ Data Loss Prevention (DLP) Software ensures end users do not send sensitive or critical information outside of your corporate network and provides reporting to meet certain compliance and auditing requirements.

- ✓ Configure 'External Mail' warning messages to identify mail originating from outside of your organization & to help end users thwart potential phishing attempts.

- ✓ Ensure that you have a webmail portal. Receiving and sending email in the event your primary mail is unavailable will allow you to continue business operation should you experience an outage of your primary mail system.

Regain Confidence In Your IT Support Today!