Cyber Risk For Startups

Tara Spalding
Managing Director, BoomStartup Accelerator
www.boomstartup.com
https://www.linkedin.com/in/taraspalding/

Your Startup Is At Risk

Everyone is a target, unless you do business that is 100% offline.

Over 2,000 cyber attacks happen every day, approximately one attack every 30 seconds.

Cyber attacks happen through every communication channel. Phone calls, texting, social media, website, email, snail mail, etc - so everyone at your startup or who has access to your internal systems, servers, network must be aware that they are the exposure point to criminal activity.

Focusing on cyber risk and coming up with process, protocol, and practice for your startup will reduce exposure. Most improvements can be done for no or low cost.

Additional support such as software, hardware, consultants, insurance can further reduce risk.

Threat Landscape

Phishing, Spear Phishing, Vishing, Smishing	Tricking employees, contractors, customers into sharing sensitive information.
Social Engineering, Disinformation, Pretexting	Bad actors impersonating people in control to find information, get access into systems or extort money.
Spyware, Malware, Bot, Malicious Apps, Ransomware	Programs that corrupt, scramble, block access to systems or data usually repaired by ransom payment.

Protect by Practice

Get employees and contractors into habits of suspicion and double-check before acting.

- Periodic training on cyber threats
- Identify if sources are trusted or not
- Implement scans of downloads, apps, attachments
- Understand that attacks happen through email, phone calls, texting, social media
- How and Who to communicate when suspicious activity occurs
- Cultivate encouragement vs. shame to share when situations happen (don’t hide if something bad happens)

Protect by Protocol

Get employees and contractors to use authentication and safe networks

- Routine password changes
- Company authorized password storing systems (lastpass)
- Company authorized VPNs, hotspots
- Email scans, whitelisted accounts
- Two-factor authentication, Three-factor authentication
- SaaS application authenticators
- File upload and download scans from directory and file management solutions
- Data storage and location protocol

Protect by Process

Get employees and contractors to understand what to do when any stranger asks them for something.

- Process on validating person, source
- Read domain names, email addresses, phone numbers
- Do not use the number or contact given yet find a public phone number, website address before responding
- Report suspicious activity so others in your company don’t fall prey to the scam