2 ways **cybercriminals can breach** your health care organization

And 3 ways to **RUIN THEIR CHANCES**

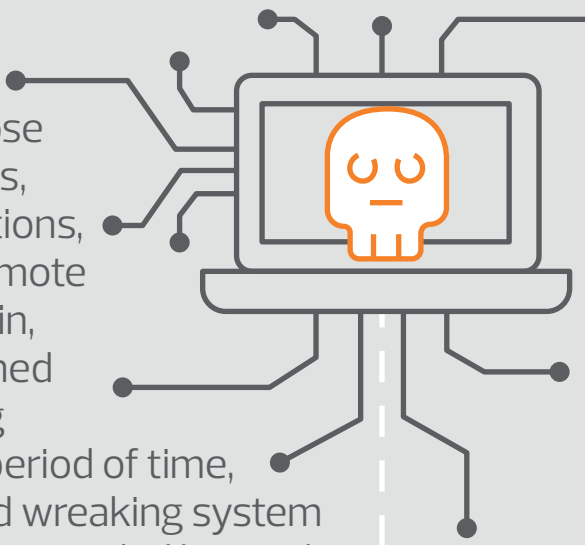
What should you and your health care organization be watchful for and how can you mitigate these cyber risks?

2 WAYS BAD ACTORS BREAK IN

1

REMOTE WORKFORCE

Remote workers unwittingly can expose their organizations via phishing emails, ransomware, vulnerable storage locations, as well as compromised employee remote networks or personal systems. Once in, cybercriminals can hang out in breached systems, often undetected, gathering organizational and patient data for a period of time, eventually capitalizing on the data and wreaking system havoc. The enterprise environment is extended beyond the walls of the traditional hospital.



2

THIRD-PARTY PROVIDERS

Vendors and partners provide valuable resources and additional services to health care organizations; however, if data is not secured in a consistent manner from system to system, this signals a potential risk opportunity. Third party access control should be assessed and managed to prevent unwanted elevated access. Cybercriminals are always looking for that break in the system.

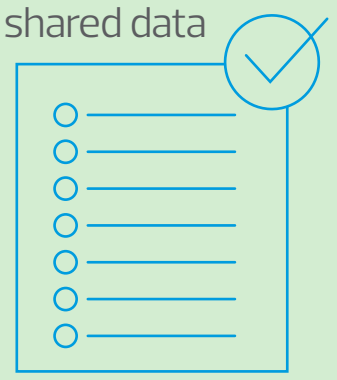
3 WAYS TO KEEP THEM OUT

GENERAL RISK ANALYSIS

This analysis measures data storage, access controls, security policies, governance, antivirus protection, incident response planning, liability insurance and more. The key to addressing cybersecurity risks is understanding security needs as early as possible and communicating risks effectively up and down the organization. This analysis helps organizations form the baseline to mitigate vulnerabilities.

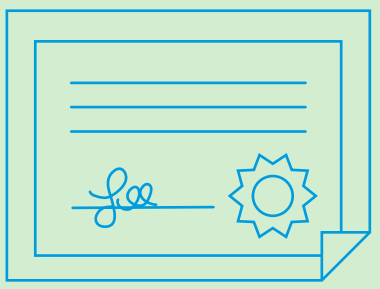
REMOTE WORKFORCE ASSESSMENT

This assessment focuses on employee tools, solutions, controls, shared data processes, virtual private networks, regulatory considerations and more. Tabulating a risk registry of possible exposures and frequently evaluating those concerns are key.



FRAMEWORK CERTIFICATION

Aligning to a security framework, like HITRUST, that fits organizational requirements can be an effective way to mitigate cyber risks. Performing a gap analysis against what the requirements dictate and what the health system has in place can provide an excellent baseline for the organization. Receiving an attestation of compliance to a framework can also provide a market differentiator showing how seriously the organization takes security.



Best practice for a dedicated security budget is between 5% to 10% of the IT budget; however, many organizations may spend significantly more to battle cyber vulnerabilities. RSM can work with you and your health care organization to determine where you should focus your cybersecurity next steps to help prioritize financial implications and resources. Our security, privacy and risk consulting professionals have deep experience in the health care industry as well as cybersecurity strategies.

CONTACT US to learn more.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

ig-nt-ras-hc-1120_health-care-cyber-infographic