Terrifying Technology Tales™

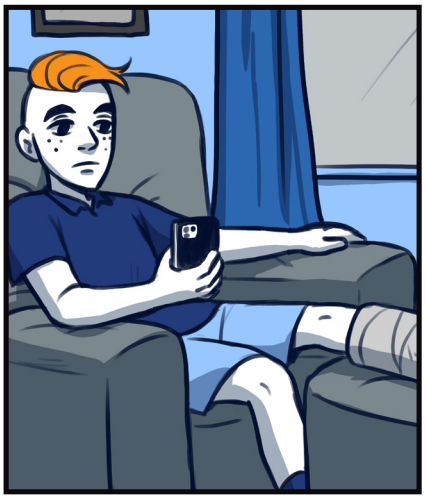
VOLUME 2, ISSUE 1.

VISUAL EDGE IT™
SECURE TECHNOLOGY SOLUTIONS

CONTENTS

GONE MISSING

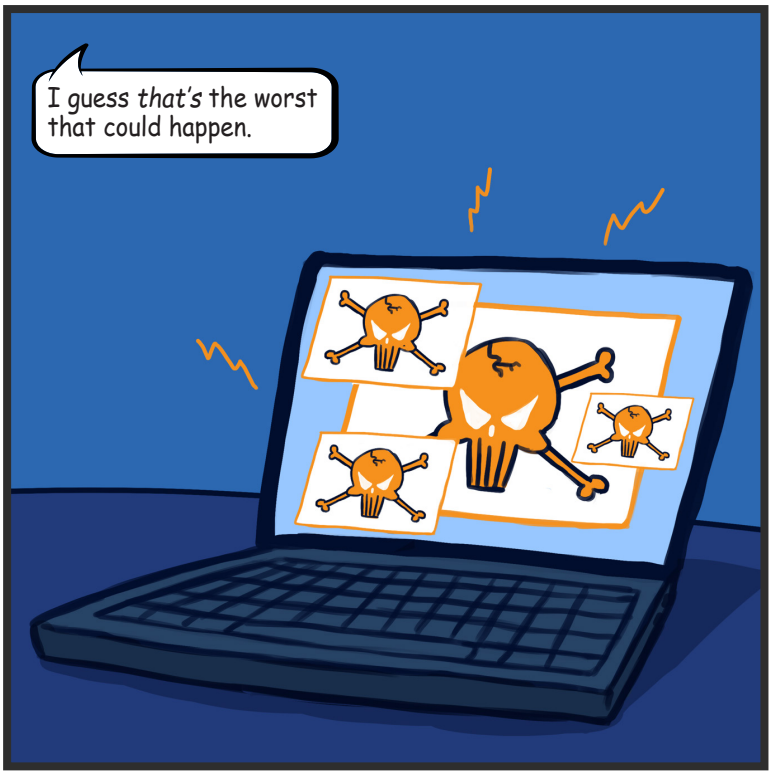
A quiet server room. An unsuspecting business. And a cursor found moving about freely in the dark! Hear the creepy, nail-biting tale of a family- owned business' struggle to get their company data back from cyber criminals.



HORROR HOSPITAL

A hospital decides to stick with their local managed services provider instead of choosing Visual Edge IT™. Later, a patient's personal information is threatened by hackers. Talk about adding insult to injury.

GONE MISSING



IT SUPER KNOWLEDGE

START WITH THESE STEPS

IT Assessment

A network assessment will identify security vulnerabilities. This can easily be conducted by a trusted advisor/IT partner. Your provider will make recommendations to increase security and reduce cyber threat risks.

Backup Disaster Recovery Plan

Having a great disaster recovery plan in place can significantly minimize downtime and recovery. If a ransomware situation does happen, you are able to recover quickly along with not having to pay the ransom.

Advanced Endpoint Security

Advanced endpoint security uses artificial intelligence to identify and prevent known and unknown threats in real time. Devices are able to self defend by stopping processes, quarantining those processes and notifying the Security Operations Center to start file rollback.

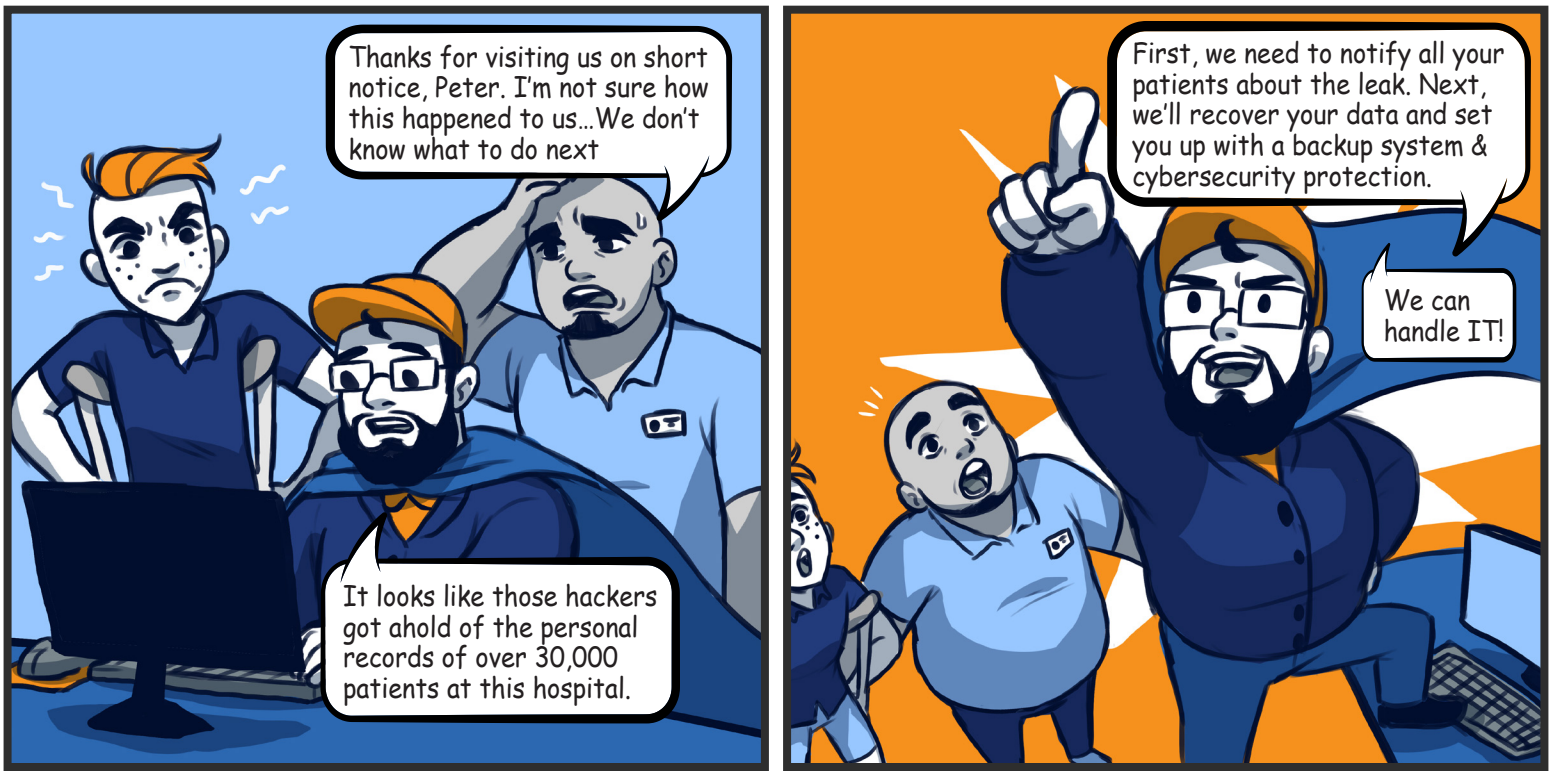
Security Operations Center (SOC)

You should choose an IT partner who provides a Security Operations Center that is well integrated with the end user service desk. The SOC watches 24/7 for global cyber security threats and advises the service desk of any issues. The service desk can take proactive actions to alert and protect their customers from cyber criminals.

To learn more about how to protect your organization, check out these additional resources.

- Network Security Checklist
- Ransomware Checklist
- Solutions for Backup & Recovery

HORROR HOSPITAL



IT SUPER KNOWLEDGE

START WITH THESE STEPS

Managed IT Services

A Managed Service Provider (MSP) can alleviate stressors for healthcare systems by offering a broad range of support. MSPs can help monitor patient data and minimize factors that may lead to HIPAA violations, including:

- **Untrained Employees:** An untrained employee is a significant liability for any organization. Losing a patient's information or unknowingly passing it on to outsiders and non-covered entities can result in severe penalties.
- **Theft or Cyberattacks:** The most unfortunate way of violating the HIPAA is to lose the patient's identifiable data, either due to theft or a cyberattack. This is where ensuring cybersecurity by MSPs comes into play.
- **Unencrypted Data:** While encryption isn't mandatory under HIPAA, unencrypted data is highly exposed to breaches and attacks.

Security & Recovery Plan

Healthcare organizations and hospitals must have security and recovery plans in place—not only to meet HIPAA compliance regulations but make sure that the risk of security breaches is minimal.

Cloud Computing

Cloud service providers such as Microsoft Azure have taken precautions to ensure that Protected Health Information (PHI) is protected and contract with organizations, setting limits on how they manage PHI.

To learn more about how to protect your organization, check out these additional resources.

- HIPAA Security Checklist
- A Quick Guide to Managed Security
- Breach Risk Prevention Checklist

Reach out anytime to ask a question or to schedule a no obligation IT security review.

www.visualedgeit.com
(866) 863-2266

VISUAL EDGE IT™

SECURE TECHNOLOGY SOLUTIONS

Written by Sam Lahey. Illustrated by Cassidy Rivers. Layout by Michelle Bates.