Visual Edge IT™

# Terrifying Technology Tales™

Volume 2, Issue 3.

# CONTENTS

# TERRIFYING TECHNOLOGY TALES

## THEY'RE HERE

A small architecture and engineering firm is visited by ghosts – err, hackers – in their outdated computers. At first, the old PCs appear unassuming, and the partners transfer content to the cloud before the relics are replaced with new computers. The situation turns nasty when the the system spooks terrorize the firm and "disappear" their vulnerable customer information. Will the team of paranormal PC investigators, be able to face down the apparitions and retrieve the missing data?

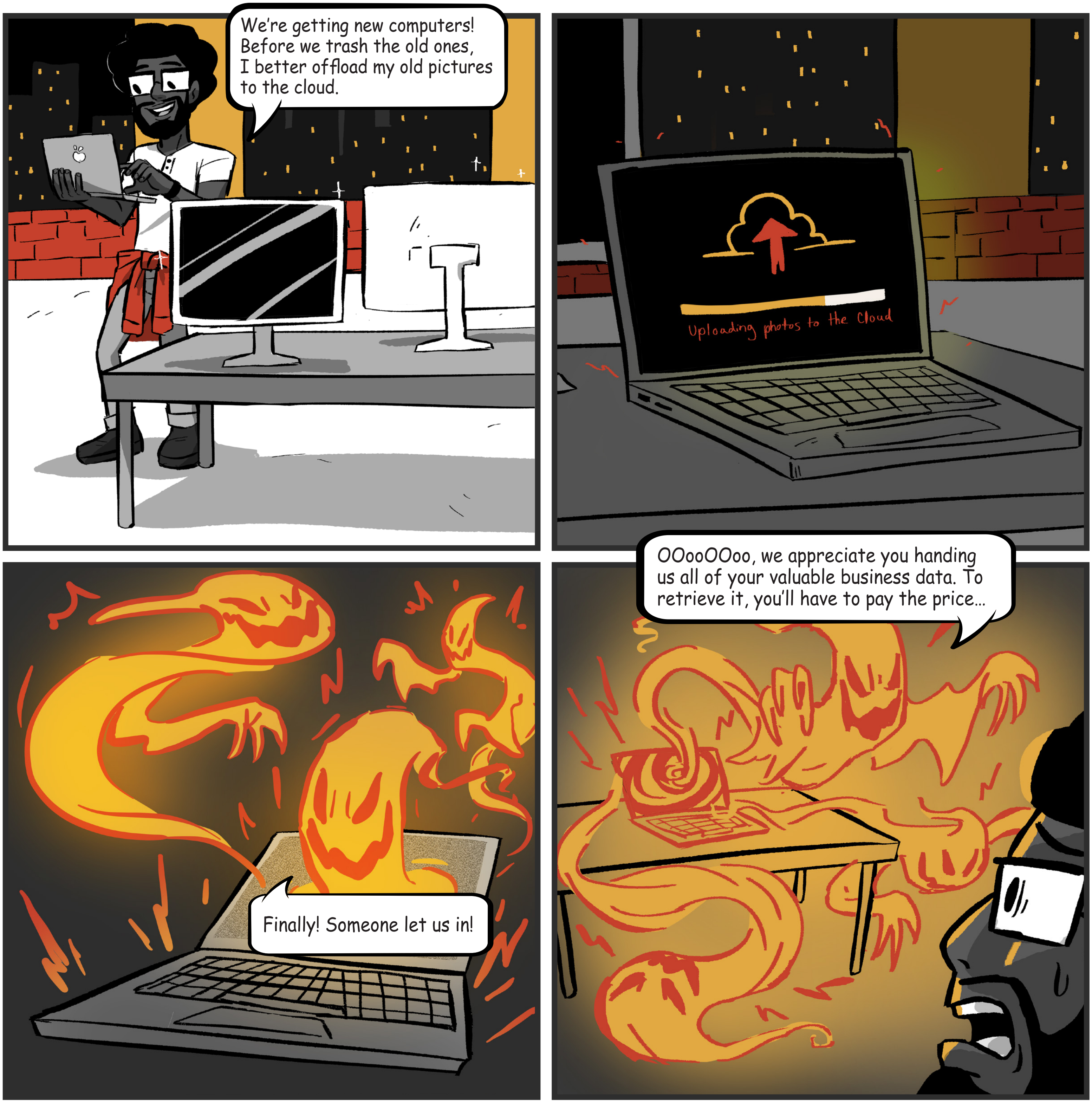
## HACKBUSTERS

Are you doing enough to thwart hackers' interdimensional malevolent plans? Multi-Functional Printers (MFPs) are a gateway to another, more sinister dimension – a doorway that digital demons will use to release evil upon on your network. Though the news has been out for years, too many businesses remain unaware of the threat lurking beneath the surface. Your printer may be possessed, and a new era of evil can be visited upon your network. Who you gonna call?

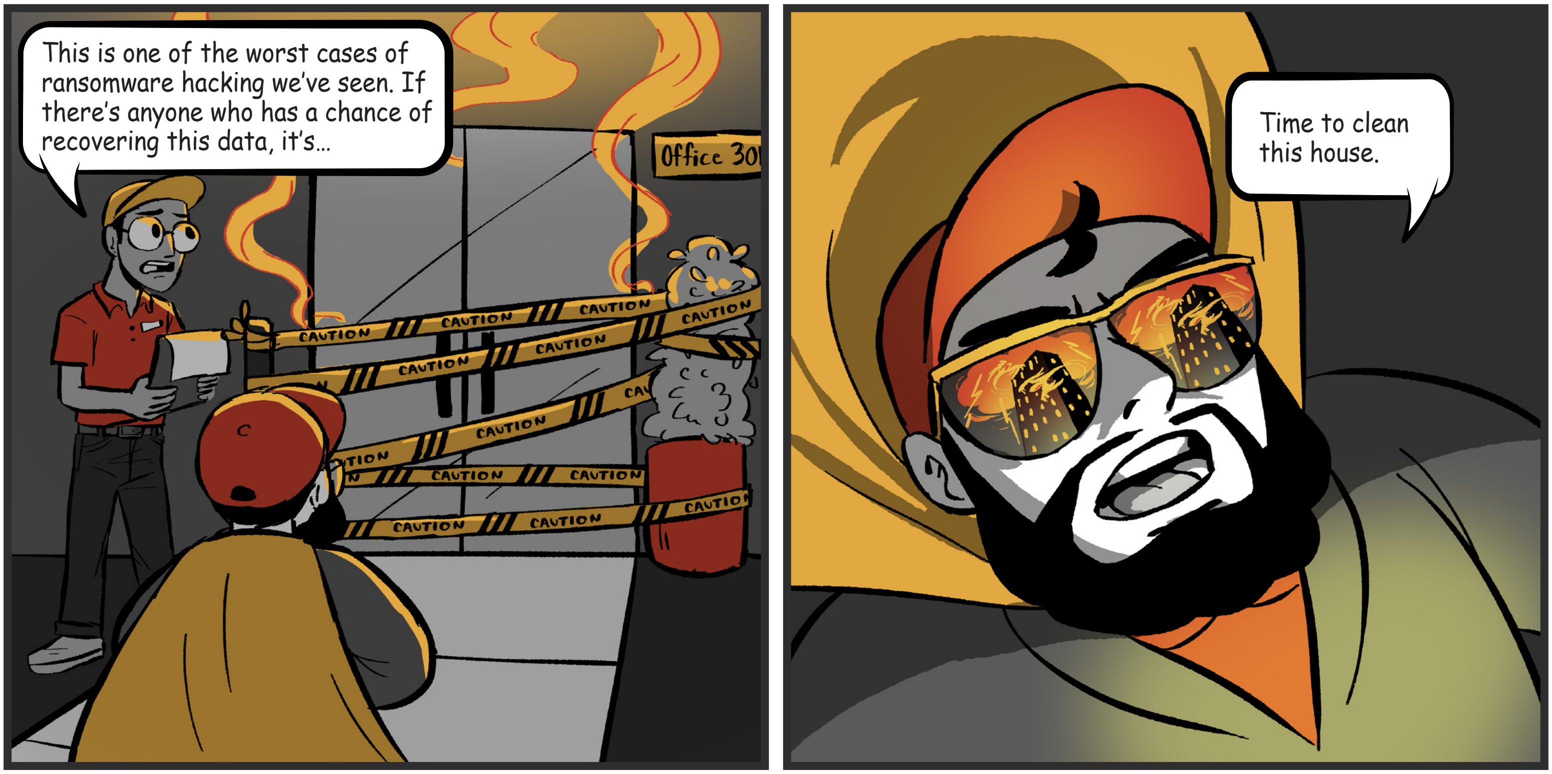
## DEADLY DESKTOP DEMON

In the far reaches of an unsuspecting network, a cybersecurity crew on-boards a device until they receive a distress call... an alien one. Unknown to them, they will soon encounter the most terrifying creature in the universe: The Ransomware Hacker. Find out what happens when a hacker infiltrates an entire company via a remote desktop protocol, allowing the deadly desktop aliens to bypass all protection systems. All alone in cyberspace, no one can hear you scream...

# THEY'RE HERE...


We're getting new computers! Before we trash the old ones, I better offload my old pictures to the cloud.
Uploading photos to the Cloud
Finally! Someone let us in!
OOooOOoo, we appreciate you handing us all of your valuable business data. To retrieve it, you'll have to pay the price...

© Visual Edge IT. All rights reserved.


This is one of the worst cases of ransomware hacking we've seen. If there's anyone who has a chance of recovering this data, it's...
Office 30
CAUTION
Time to clean this house.

# IT SUPER KNOWLEDGE

## START WITH THESE STEPS

### Have a 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. Minimizing downtime during restores needs to be considered when evaluating a backup process.

### Beware of Outdated Hardware or Software

Hardware and software have lifespans and can only last for so long. Continuing to operate hardware or software that is outdated or not supported can create a huge hole in a company's security. Installing patches and updates is essential, but when support ends, so do the updates and patches.

### Conduct Employee Cybersecurity Training

Employees are the first line of defense when it comes to network security. Making employees aware of security risks and showing them ways to recognize a possible attack and how to defend them is one of the best methods of stopping an attack before it happens.

### Perform a Security Risk Assessment

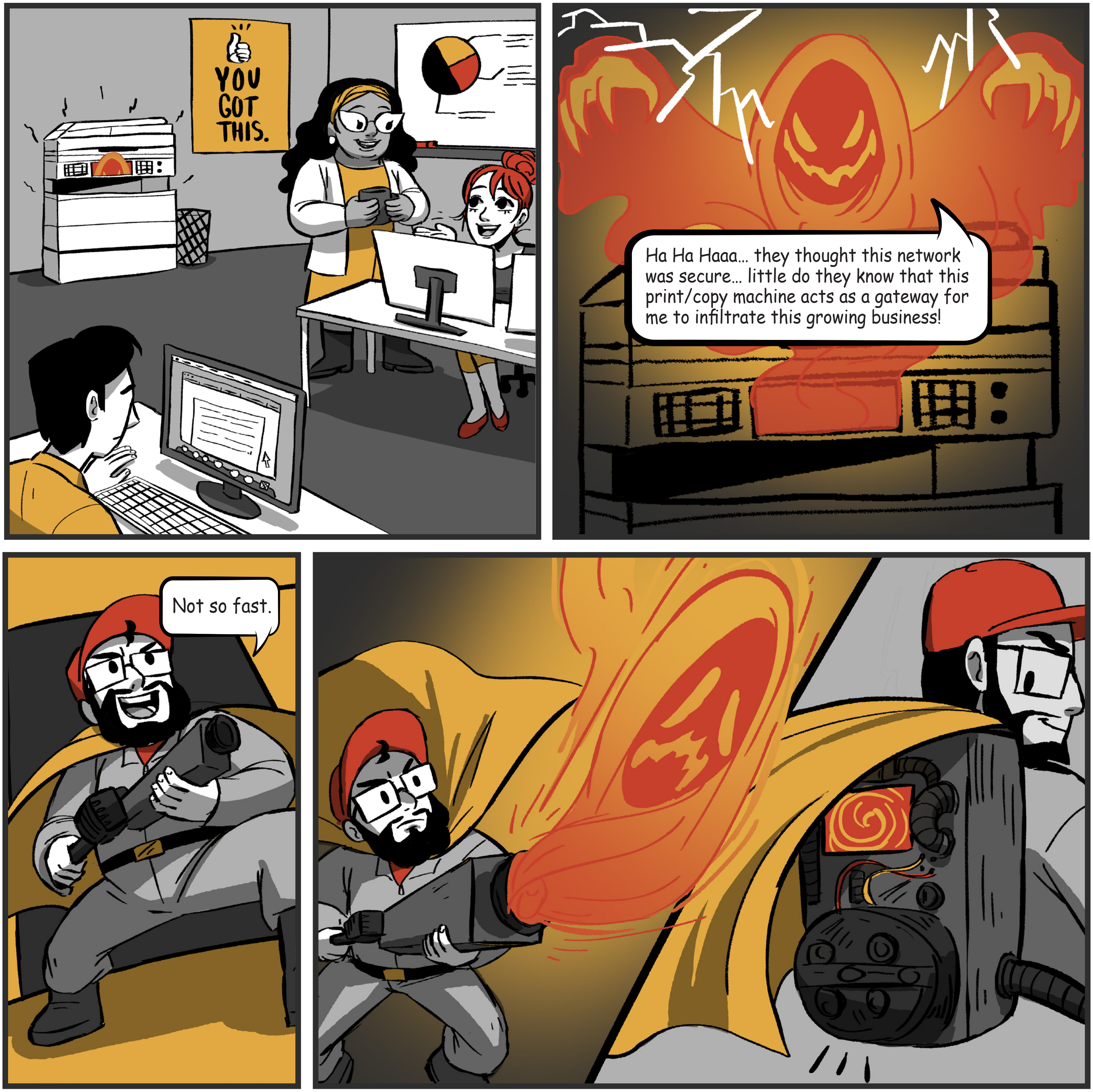
Having an assessment will determine what safeguards should be in place that are currently not.

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

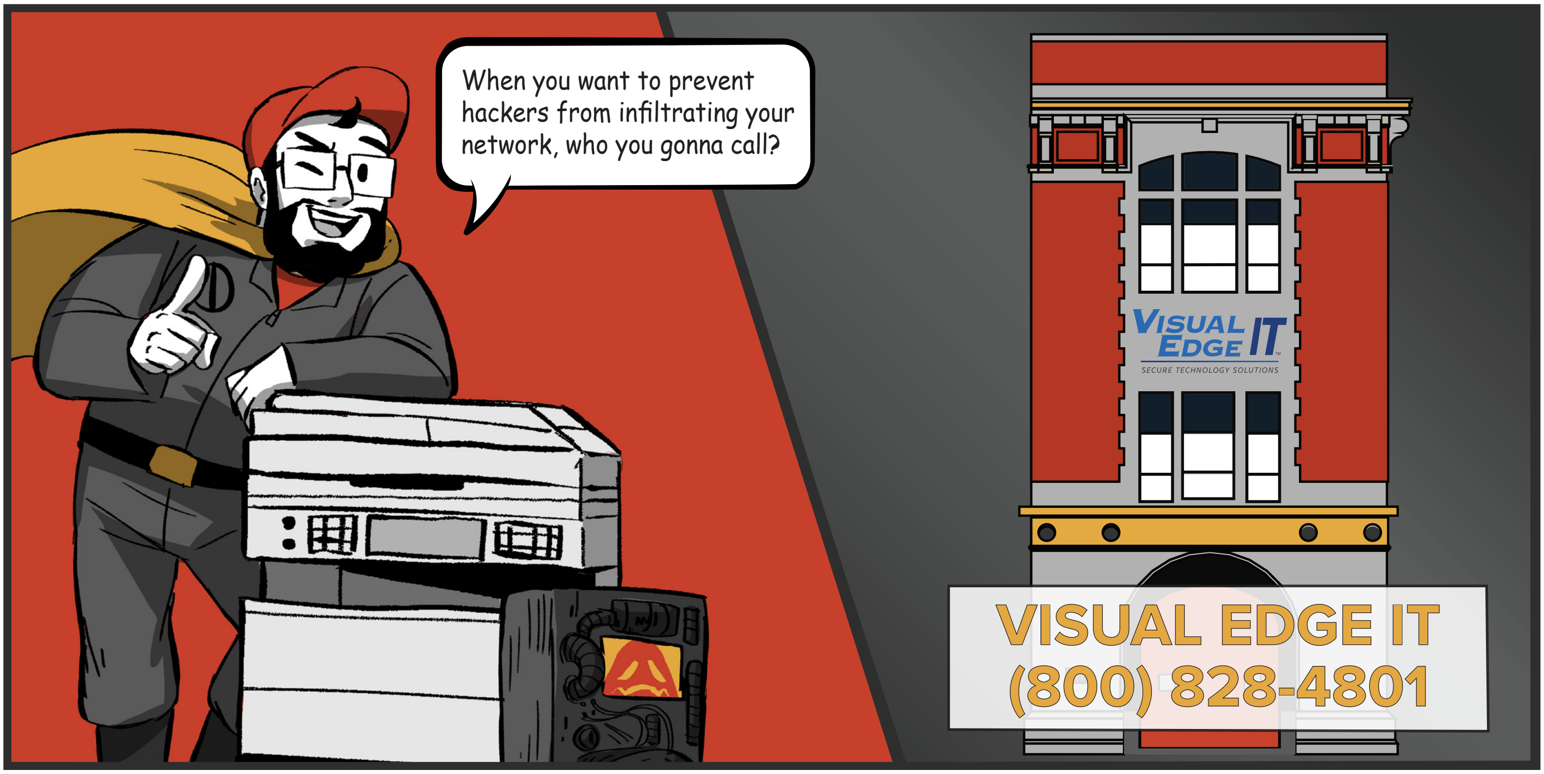
- Quick Guide to Ransomware Defense
- Quick Guide to Backup and Recovery
- Quick Guide to Managed IT Services

© Visual Edge IT. All rights reserved.

# HACKBUSTERS


YOU GOT THIS.
Ha Ha Haaa... they thought this network was secure... little do they know that this print/copy machine acts as a gateway for me to infiltrate this growing business!
Not so fast.

© Visual Edge IT. All rights reserved.


When you want to prevent hackers from infiltrating your network, who you gonna call?
VISUAL EDGE IT
SECURE TECHNOLOGY SOLUTIONS
VISUAL EDGE IT
(800) 828-4801

# IT SUPER KNOWLEDGE

## START WITH THESE STEPS

### Treat Multi-Functional Printers Like Computers

Data breaches are not restricted to “traditional” targets like PC’s or mobile devices. Any network connected device is a potential risk. Include print devices in your security plan.

### Conduct Printer Security Assessment

Evaluate your equipment and know what the vulnerabilities are with each machine. Printers that are connected to the internet create a higher risk for a data breach. Identify what access is available on each printer and who has access.

### Encrypt/Wipe Stored Data

Encrypting stored data on printers ensures that data is secure and isn’t accessible if there’s an unauthorized breach. Periodically wipe or overwrite hard drives when printers are stored are no longer used.

### Partner with a Managed Print Services Provider

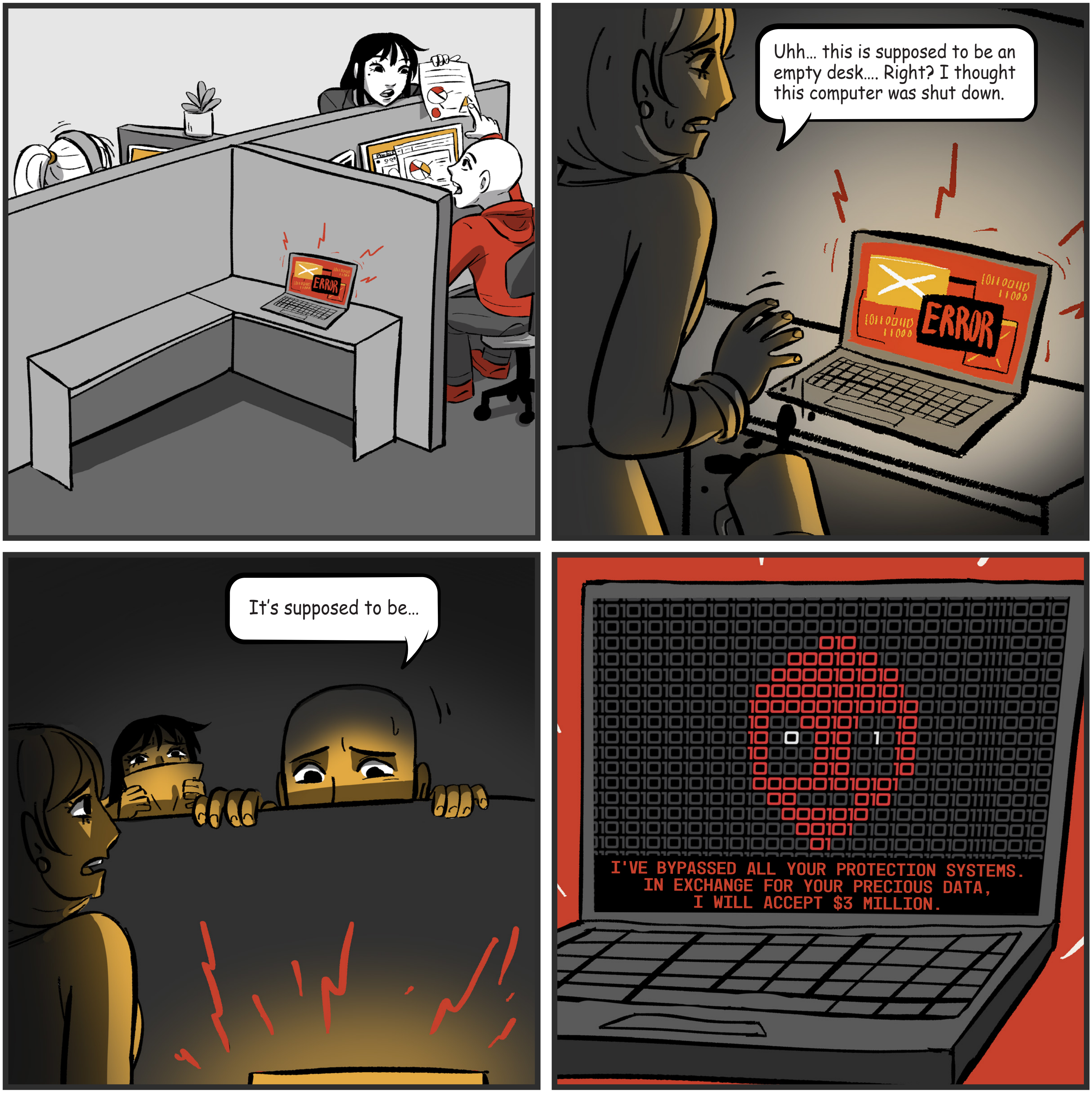
Companies with limited personnel and skill will often rely on managed print service providers to assist with evaluating, monitoring, or managing their printers and printer security.

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

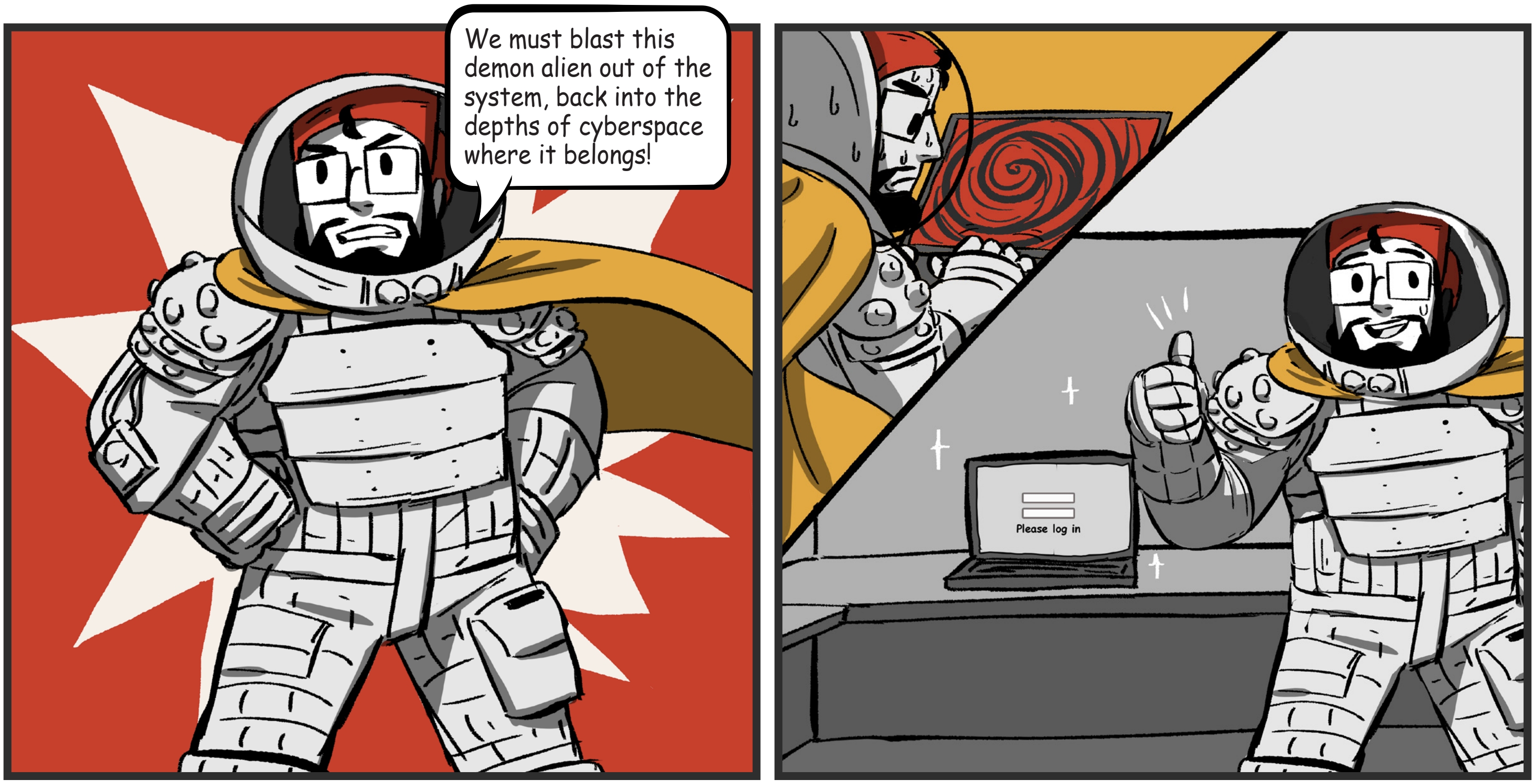
- Printer Security Plan Checklist
- FTC Safeguards Rule Checklist
- Network Security Checklist

© Visual Edge IT. All rights reserved.

# DEADLY DESKTOP DEMON


ERROR
Uhh... this is supposed to be an empty desk.... Right? I thought this computer was shut down.
ERROR
It's supposed to be...
I'VE BYPASSED ALL YOUR PROTECTION SYSTEMS. IN EXCHANGE FOR YOUR PRECIOUS DATA, I WILL ACCEPT $3 MILLION.

© Visual Edge IT. All rights reserved.


We must blast this demon alien out of the system, back into the depths of cyberspace where it belongs!
Please log in

# IT SUPER KNOWLEDGE

## START WITH THESE STEPS

**Security Patches, Updates, and Programs**
To stop ransomware from breaking into a network infrastructure, a company needs to be diligent in keeping its implemented software completely updated. Many times, viruses will sneak past security safeguards through gaps in unpatched application security protocols. Hackers are always hunting for the security loopholes caused by outdated software and operating servers, and target weaknesses in IT infrastructures. Regularly updating your business software can eliminate these vulnerabilities.

**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.**

- Breach Risk Prevention Checklist
- Ransomware Checklist
- Quick Guide to Data Recovery

© Visual Edge IT. All rights reserved.

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

**www.visualedgeit.com**
**(800) 828-4801**

VISUAL EDGE IT TM

SECURE TECHNOLOGY SOLUTIONS

© 2022 Visual Edge IT. All Rights Reserved.