



RevITup™ TechEd Cloud Webinar Series

Security Unmasked

Exposing the Technology Monsters Hiding in your Business



Date: October 30, 2014

Time: 12:30 PM - 1:30 PM

Location: Online Webinar



Presented By
Ilene Rosoff, CEO The Launch Pad

RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY





The Launch Pad – Welcome to the New Face of IT

About The Launch Pad

The Launch Pad provides fixed-fee managed technology and web services to small and mid-sized businesses. With our **RevITup™ Business Care Technology and SilverCloud Series**, our clients enjoy a monthly fee that never fluctuates regardless of the number of service requests. That means we never profit when your systems are down. Our goal is nothing short of a dramatic reduction in the cost of technology ownership and in your technology-induced stress level.

- Founded in 1992, Offices in Tampa Florida
- IT Management, 24x7x365 Help Desk, Network Integration, Data Protection, Cloud Services
- RevITup Business Care™ Managed Technology Series, Professional Services & Sales
- **RevITup SilverCloud Series™** ; VirtualGreen Office™, Hosted Applications, Web Services
- 2009 , 2010, 2011 & 2012 Inc. 5000, Tampa Fast-50 fastest growing companies & MSP 100
- 2009, 2010, 2011 CEO Ilene Rosoff Named Finalist for the Tampa Business Woman of the Year
- 2012 – Launch 1st National managed IT franchise offering





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

The delivery system for business technology has undergone a paradigm shift in the last 5 years and there is no going back.

What's Lurking in Your Business:

- Nearly 50% of data breaches or loss came from accidental exposure, employee intent or lost/stolen PCs and smart devices.



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

What's Lurking in Your Business:

- In a 2014 survey by Symantec, 42% of businesses said they lost confidential data in the last 12 months and 40% reported a direct financial loss because of this.





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

What's Lurking in Your Business:

- 1 in 8 legitimate websites have a critical vulnerability.



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

What's Lurking in Your Business:

- 2013 is Deemed the Year of the Mega Data Breach. 552 million identities were exposed - up more than 500% from 2012.



**These attacks hit some of our largest corps with extensive IT resources at their disposal.





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

What's Lurking in Your Business:



- 66% of SMBs were confident that their data and devices are secure and safe from hackers. 77% said they had not been hacked.



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

However in Reality...

- Targeted attacks destined for small business (1 to 250 employees) accounted for 31% of all attacks last year, compared with 18% in 2011.





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

Many Small Business Owners Want to Know, What's Changed?

- Everything is online & technology is untethered
- BYOD – Employees are using their own devices
- Hacking is BIG Business; not for kids anymore
- Management lacks attention to detail & tech policy
- Ignorance of the true nature & extent of threats

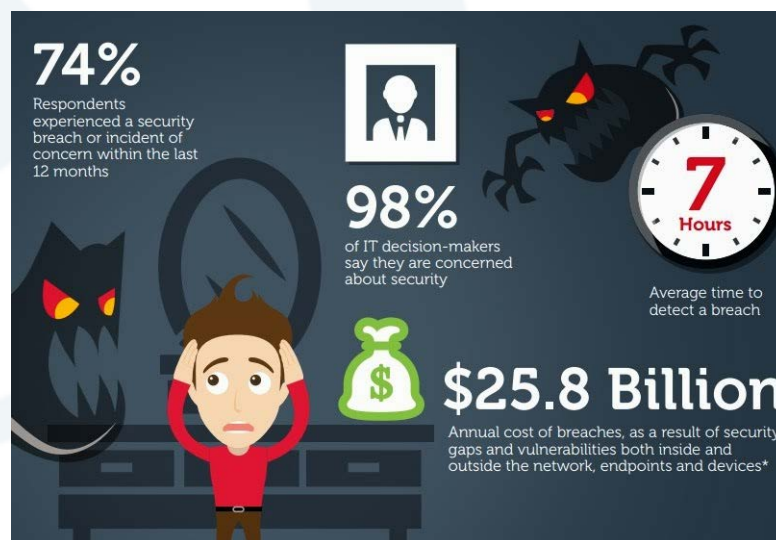




Security Unmasked

Exposing the Technology Monsters Hiding in your Business

**The Bigger Question is,
What Can You Do About IT?**



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY





Security Unmasked

Exposing the Technology Monsters Hiding in your Business

Goals for Today

1. **Expose the 5 Top Security Vulnerabilities:** We will identify the hidden dangers in your environment that you likely don't know about. Some may surprise you.
2. **Identify the Common Traps in Protection:** Many businesses are lulled into complacency with tools like standard antivirus or data backups. Knowledge is power. We'll show you why this isn't enough in today's technology landscape.
3. **Detail 5 Surefire Tools You Need to Know About:** Today we will illuminate 5 tools every small business should know about to counter these threats.
4. **Provide a Security Template Practical for SMBs:** Nothing is 100% foolproof in today's fluid technology environment but this template can help shut down the most serious vulnerabilities.





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

5 Top Security Vulnerabilities Unmasked

1. The Physical Space

Horror stories abound about business-class servers sitting in tiny closets with no ventilation. We've even seen network racks in bathrooms. Infrastructure that lacks proper wiring, racking, cable management and power management leave your business vulnerable at the most basic level to accident, sabotage and unnecessary wear and tear.



Best practice physical space planning and executions is one of the most neglected technology management components in small business. It can also be one of the most costly. **Proper planning, wiring, cooling, housing and power protection is absolutely essential to protecting your business!**





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

5 Top Security Vulnerabilities Unmasked

2. BYOD – Stolen, Lost & Compromised Mobile Devices

Remember when a Department of Veterans Affairs' employee's laptop was stolen from his home. The laptop contained 26.5 million veterans' medical history. How can you make sure this does not happen to your business?



Password protect all mobile devices. Encrypt data when transporting it anywhere on a mobile device. Create and enforce policies for employee BYOD and company mobile devices, what can they access and store; how are devices managed - MDM, what happens when an employee leaves the company or a device is lost or stolen.





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

5 Top Security Vulnerabilities Unmasked

3. Malvertising (or... how did my protected PC get infected?)

One of the most common questions we get asked is, "We have AV protection, our email is screened, we don't install software.

So, why are users still getting infected?"

The answer is "Malvertising". This involves injecting malicious or malware laden advertisements into legitimate online advertising networks and webpages. Clicking on these advertisements can infect a PC.



Along with antivirus and malware protection, Ad Block add-ons can be installed through a browser. Even better, Web Content Filtering software and appliances offer another layer of protection. These tools filter websites and ads to offer your business safer web surfing.





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

5 Top Security Vulnerabilities Unmasked

4. Multi Function Printers

Only 6% of businesses surveyed saw MFPs as a security threat. That is a false sense of security. With Cloud printing, an attacker can create a malware app that infects the mobile device, attaches itself to a cloud print job, and gets downloaded to a networked MFP. That print job can completely bypass a firewall and infect an entire network. MFPs have hard drives and store jobs. A decommissioned MFP not data-wiped could provide easy access to confidential data unwittingly stored on the hard drive.



MFPs need passwords and planned disposal. Wireless and Cloud printing should be turned off or tightly managed. Printing policies and printer location needs to be considered including who has access to produce and receive printouts, email and faxes. Manage network printers via a server.





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

5 Top Security Vulnerabilities Unmasked

5. Online/Cloud File Sharing Services

DropBox, Google Drive, Evernote... Do you know what file sharing services employees are using on your network? SMB employees are often adopting unmanaged, personal-use online file sharing solutions without IT management or knowledge. Rogue, online file sharing poses a huge security and compliance risk to your organization and its data.

SMB's need to establish and enforce a file-sharing policy. Offer a standardized online file-sharing solution that offers real security like Citrix File Share. Classify documents, limit users and standardize to one approved service. Free is not really free. The cost to your business of unmanaged file distribution can be high.





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

Identify the Common Traps in Protection:

Don't be lulled into complacency with tools like standard antivirus or once-a-day file backups. Knowledge is power.



What Are 3 Top Protection Traps Lurking in Your Business?



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY





Security Unmasked

Exposing the Technology Monsters Hiding in your Business

3 Top Protection Traps Lurking in Your Business

1. Unmanaged File-Based Data Backup



The WORST set a once-a-day data back up ... and think you're safe. Unmanaged backups will fail. File-based backups won't restore a server or correctly backup databases. Data Protection is a strategy that includes real-time, imaged backups, managed, monitored systems and offsite and onsite storage for comprehensive recovery. The key is not the backup. It's BULLET PROOF DATA RECOVERY.



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

3 Top Protection Traps Lurking in Your Business

2. Unmanaged Employees

- 54% of employees don't follow IT policies
- 33% are not even aware of policies



Implementing security policies, educating your employees and enforcing those policies are 3 of the most effective steps you can take to protect your business and secure your business's technology. One rogue or careless employee can wipe out the most well-designed and managed technology system.



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY



Security Unmasked



Exposing the Technology Monsters Hiding in your Business

3 Top Protection Traps Lurking in Your Business

3. Unmanaged Devices and Networks

The best security and protection is achieved through visibility and access. If end-user devices and network resources can be monitored and managed, the chances of data breach, unauthorized access, compromise or loss can be greatly reduced.



Even in the event that a vulnerability is exploited, managed IT Service providers can provide the tools and expertise needed to quickly mitigate potential risks.



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

5 Surefire Tools/Tips to Arm Your Business

For small businesses with relatively limited technology resources, the challenge can seem overwhelming. Targeted vigilance is essential to your survival. These tools will go a long way toward that goal without breaking the bank



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY





Security Unmasked

Exposing the Technology Monsters Hiding in your Business

5 Surefire Tools/Tips to Arm Your Business

1. SANS - Information Security Policy Templates

<http://www.sans.org/security-resources/policies/general#acceptable-use-policy>

A written security policy is the best way to clearly identify best practices for internal and remote users. SANS offers great, free security policy templates. However, it's not enough to just have a policy, you need to review the policy with your users and make sure they understand why you expect them to follow the guidelines. Integrate security policy training into your new hire and training processes and review it periodically so every employee knows the best security practices for your organization.





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

5 Surefire Tools/Tips to Arm Your Business

2. **Tripwire SecureScan™, a free, cloud-based vulnerability management service**

<http://www.sans.org/security-resources/policies/general#acceptable-use-policy>



This organization offers a free scanning service for up to for up to 100 devices (IPs) four times a month. This tool makes vulnerability management – a widely recognized security best practice among large corporations – easily accessible to SMBs that do not have the resources for enterprise-grade security technology. Have your IT department or company do this for you.





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

5 Surefire Tools/Tips to Arm Your Business

3. Multi-tiered Real-time System of Intrusion Tools

Antivirus and a Firewall are no longer enough to protect against the exterior threats to network intrusion or infection. A managed system that incorporates layers is the only effective protection.

1. Business-class Firewall
2. Managed Anti-virus and Anti-malware on Servers and Workstations
3. Integrated Anti Spam Service, Software or Appliance
4. Web/Internet Content Monitoring & Filtering System
5. Lock Down Wi-Fi & Password, Password, Password





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

5 Surefire Tools/Tips to Arm Your Business

4. Internal Controls

75% of all successful security incidents are launched and perpetrated from inside of a company. This staggering figure increases to 86% when you focus on businesses with fewer than 250 employees in non-regulated industries. Completing a few simple (and free) steps goes a long way.



1. Require passwords to be changed regularly (most networked computers can do this automatically for you)
2. Control what users can access what data that is shared across the network
3. Place your server(s) in a locked room and carefully control who has access to that room.
4. Regularly audit and assess what system settings and business procedures have changed internally to ensure you stay protected.





Security Unmasked

Exposing the Technology Monsters Hiding in your Business

5 Surefire Tools/Tips to Arm Your Business

5. Know Where Your Data & Devices Are at ALL Times

That Means:

1. No Rogue Online File Sharing Services
2. Policies and protections for document printing/output – Particularly MFPs
3. No unauthorized use of external drives or USB Sticks
4. Monitored mobile devices that can be accessed or wiped if compromised
5. Email retention to back track outgoing file attachments.
6. Managed remote access and audited file copy abilities.



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY





Security Unmasked

Exposing the Technology Monsters Hiding in your Business

A Practical Security Template for SMBs

3 Part Security Assessment Template

While nothing is 100% foolproof in today's fluid technology environment, this 3-part template will help you prioritize your protection needs and pinpoint the most serious vulnerabilities:

1. Identifying and prioritizing your organization's information types
2. Identifying the protection needed based on priority
3. Estimating costs from bad things happening to your important business information





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

A Practical Security Template for SMBs

1. Identifying and prioritizing your organization's information types:

1. Make a list of all the information types used in your organization.
2. List & prioritize the 5 most important types of information used in your organization.
3. Identify the system on which each information type is located.
4. Complete table for all your business information types – in priority order.

Priority	Type of Information	Stored on What System
1.		
2.		
3.		
4.		
5		





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

A Practical Security Template for SMBs

2. Identify the protection needed based on priority

1. Think about the information used in/by your organization.
2. Enter the 5 highest priority information types
3. Enter the protection required for each information type in the right 3 columns.
(C – Confidentiality; I – Integrity; A - Availability) <"Y"-needed; "N"-not needed>
4. Complete the table for all your business information types.

Priority	Type of Information	C	I	A
1.				
2.				
3.				
4.				
5				





Security Unmasked

Exposing the Technology Monsters Hiding in your Business

A Practical Security Template for SMBs

3. Estimate costs from bad things happening to your important business information

	<data type name> Issue: Data Released	<data type name> Issue: Data Modified	<data type name> Issue: Data Missing
Cost of Revelation			
Cost to Verify Information			
Cost Of Lost Availability			
Cost of Lost Work			
Legal Costs			
Loss of Confidence			
Repair Cost			
Fines/Penalties			
Total Cost Exposure	\$	\$	\$





RevITup™ Business Care Series

Engage Our Easy-to-GreenIT™ Initiative

Sign up today for our Free Easy-to-GreenIT™ Technology Audit: www.launchpadonline.com/greenITnow

- ❖ **Incorporate Managed IT Services:** remote remediation means 90% reduction in truck rolls
- ❖ **Implement energy efficient hardware:** power management devices, notebooks instead of desktops (50% savings)
- ❖ **RevITup VirtualGreen Office™ Series** reduce TCO by as much as 50% with our packaged virtualization solution
- ❖ **Data Center/Cloud** move some or all technology hardware & software off premises
- ❖ **Renew, Reuse, Recycle** with The Launch Pad's eCycle & GreenBack™ Program



RevITup eCycle™ The Launch Pad teams with eCycling.com to recycle used equipment

Computers, monitors and other electronics contain toxic materials and occupy an estimated 70% landfills. In June 2009, The Launch Pad teamed with Computer Recyclers, a Tampa-based, national IT asset disposition and electronics recycling (eCycling) provider. Through this relationship we offer a no-cost recycling service to local companies upgrading or decommissioning equipment.

RevITup GreenBack™ GreenBack™ Nonprofit Community Outreach Program

In addition to facilitating eCycling services for local businesses, The Launch Pad's GreenBack initiative takes gently used equipment is donated by local business and repurposes it to local nonprofit organizations. If you are a nonprofit organization, you can add your "wish list" via our website's [Easy-to-GreenIT](#) signup and we will distribute equipment on a first come, first serve basis. If you are a business disposing of equipment, you can use the same form and opt to designate your equipment be recycled to a local nonprofit of choice or the next in need on our list.



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY





Security Unmasked



Exposing the Technology Monsters Hiding in your Business

Want to Optimize Security for Your Organization?

COMPLIMENTARY RevITup SilverCloud™ Security Threat Assessment

www.launchpadonline.com/SecurityUnmasked 2014 Offer Expires: **December 15th, 2014**

Sign up Today for a FREE RevITup Security Threat Assessment:

1. Review your current environment to determine the security traps in your business.
2. Provide threat prevention roadmap for locking down your technology environment.
3. If you decide that you'd like us to help you secure your technology, we will offer a **\$500 coupon** to any webinar attendee who engages our services.



RevITup™
the launchpad
WE MANAGE THE TECHNOLOGY

