IT ONDEMAND
it-on-demand.com

THE TECHNOLOGY TIMES NEWSLETTER

Inside This Month's Newsletter

JUNE 2016

This monthly publication provided courtesy of Howard Globus, Security Evangelist & Partner of **IT On Demand.**

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Shadow IT: Ignore At Your Own Risk

It's one of those little secrets that nobody wants to talk about…

The term "Shadow IT" refers to apps and devices used at work that operate outside your company's sanctioned policies and protocols.

Shadow IT takes many forms, like conversations on Facebook Messenger, Google Hangouts, Gmail or Skype. It can include software from Excel macros to cloud -based data storage apps such as Dropbox, Google Docs and Evernote. Or collaboration spaces like Slack, Asana and Wrike. And then there are devices: USB sticks, smartphones, tablets and laptops within your network that you have no control over.

Robert J. Moore, CEO of RJMetrics, relates how companies like Slack and Dropbox craft their pricing models to encourage rapid proliferation. One day, a few of his engineers were using Slack, then all the engineers, then the whole rest of the company was using it. He said, "We reached a point of no return and paying for it was pretty much our only option."

The hidden dangers of shadow IT

When users on your network adopt apps and devices outside your control, protocols aren't followed, systems aren't patched, devices get infected without people knowing it and data breaches happen… As a result, confidential information can be exposed, accounts taken over, websites defaced, goods and services stolen, and precious time and money lost.

Not only that, you end up with siloed information in unknown places, data compliance issues and missed opportunities for bulk pricing.

The obvious solution would be to crack down and forbid use of all but company-approved devices and apps. Unfortunately, that tends to slow things down, stifling productivity and innovation.

Bringing your shadow IT out into the light. Obviously, burying your head in the sand won't make the problem go away. Here's what you can do to not only take control of the situation, but actually use it to drive innovation and agility at your

Continued on page 2

company.

Cut loose the "control" mentality. It's no longer feasible to simply ban certain apps. If you don't give employees the software they prefer, they may start using their own. They can easily access a vast and growing variety of apps, all without your help – or control.

> *"Take control of high-risk situations and keep an eye on the rest."*

Recognize the delicate balance between risk and performance. Evaluate risk on a case-by-case basis. Then take control of high-risk situations and keep an eye on the rest.

Foster open communication. Get employees involved in creating intuitive policies. You can turn them from your greatest risk to your greatest asset by levering their input and ownership of protective protocols. This helps everyone maintain security while keeping practical needs for performance in mind.

Develop a fully tested plan. Even if it's only 70% complete, a tested plan will be far more useful when the need inevitably arises than a 100% complete plan that's not fully tested. Most managers underestimate the confusion that occurs in the first few days following a breach.

Unfortunately, that confusion can create a defensive rather than constructive atmosphere centered on discovering how, when and where the breach occurred. A comprehensive incident response plan can go a long way toward achieving a speedy resolution, and keep an otherwise manageable event from turning into a full-blown business crisis.

Finding the right balance. Focusing only on security and asset protection can drag down business performance quickly. However, balancing risk with performance enables you to maximize your return from investments in detection and response. It also helps you become more adept at adjusting as the security landscape changes. By developing your organization's ability to recognize threats and respond effectively to incidents, you can actually take risks more confidently and drive business performance to a higher level.

IT On Demand can help you with this. Our proprietary **Security Assessment** helps you take the friction out of data protection. Contact us today at **(212) 235-0260** or info@it-on-demand.com to take advantage of this offer (normally $297), **FREE** through the end of June, and put an end to Shadow IT in your organization finally and forever.

**Offer valid to qualified prospective clients with 10 or more computers and a minimum of 1 server.*

5 Tricks for Thwarting VoIP Threats

The VoIP market continues to grow and doesn't show any signs of stopping. As its use becomes more widespread, so too do the security threats against it. Although these type of attacks haven't received as much media attention as ransomware and phishing, they're no less dangerous or damaging to your business. Internet-based calls are far more vulnerable to fraud compared to more traditional telephony services and face threats from identity theft, eavesdropping, intentional disruption of service and even financial loss. Let's examine 5 five useful tips for protecting your VoIP network.

- **24/7 Monitoring:** A recent study indicates that 88% of VoIP security breaches happen outside of normal business hours. This can be avoided by contracting outsourced IT vendors to monitor network traffic.
- **VoIP Firewalls:** Every VoIP vendor should provide a firewall specially designed for IP-based telephony.
- **Encryption Tools:** Although some services claim built-in encryption, be sure to investigate how effective they really are.
- **VPN:** a VPN is recommended because it creates a secure connection between 2 points.
- **Password Protection:** However, in this case it actually means protecting the passwords themselves. Eavesdropping is one of the easiest, and most common, cyber attacks against VoIP networks and even with all of the protocols above, employees should be instructed to never give out any compromising information during a VoIP call.

VoIP is as important as any of your other network security considerations. It requires a unique combination of protection measures, and we'd love to give you advice on implementing any of these protections or managing your VoIP services. Give us a call today at **(212) 235-0260** to get started.

Published with permission by Techadvisory.org

Understanding and Avoiding BEC Scams

Over the last few years, the scams done through business emails have increased in an alarming number, causing companies all around the world to lose millions of dollars. Over the past two years, it has been reported that businesses have lost over 1.2 billion dollars due to these phishing attacks. Each and every situation is different from one victim-company to another, but there are similarities in these attacks which you can look for as red flags.

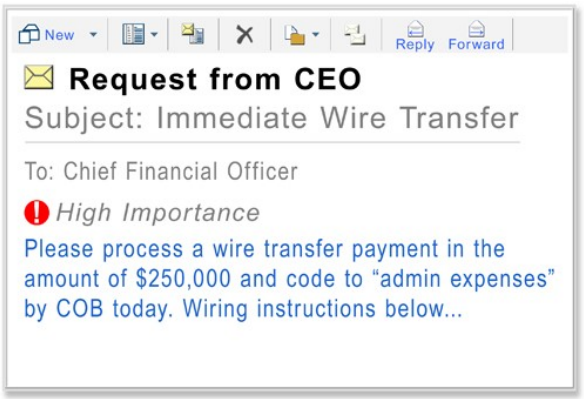
How Does BEC Work?

These cons usually begin with an innocent message over email, with the scammer impersonating a regular vendor, a position of authority within the company, or at times even posing as an attorney. After what appears to be innocuous, regular interaction over email, the fraudsters ask for sensitive information about the company in hopes that, by this time, they have already gained the employee's trust. According to the FBI, BEC deception customarily includes urgency, uses an email address very similar to the person they are impersonating, and takes place just before a holiday or weekend while the CEO is away from the office. Such emails appear to come from a trusted source about everyday business.

How to Avoid Email Scams

To avoid BEC scams, there are several steps that can be taken.

- Improve business processes. For example, confirm all fund-transfer requests prior to payment. Use two-factor authentication and require a secondary sign-off to verify any changes in vendor payment location. If using phone verification, only call verified numbers and contacts, and avoid any numbers listed in the email funds-transfer request.
- Improve Detection. Create intrusion detection rules that flag similarly structure email extensions. For example, a.manager@xyz_company.com versus a.manager@xyz-company.com.
- Manage Domain. Brainstorm and register company domains that mimic but are slightly different from your company's actual domain.
- Educate employees. It is imperative that your staff be instructed on the signs to watch for when dealing with sensitive information and financial requests. They should be kept up-to-date on the latest scams that exist nationwide. In addition, encourage your staff to ask questions or obtain the opinion of an IT professional if they have any doubt whatsoever.
- Partner with a Managed Service Provider/IT Company. To combat fraud, consider enlisting the assistance of those familiar with proper security practices. The services provided by an experienced and skilled IT company will help defend your organization against all cybercriminal activity and in turn, provide the peace of mind necessary so that you and your staff can place your focus where it should be – on your clients.



By partnering with an experienced IT company that is keenly attuned to emerging security threats, you will mitigate risks associated with such scams. **IT On Demand** can help you develop tactics and training programs that will ensure the protection of your company's assets and personnel. Call us at **(212) 235-0260** with any questions or if you would like more information. You can also feel free to email us with your requests at info@it-on-demand.com. We look forward speaking with you.

Increased Cyber Attacks on Healthcare Facilities & Businesses

As cyber attacks continue to hit different healthcare organizations, it is time for healthcare information security to up its game. Where once healthcare companies were overlooked by hackers, they have now become prime targets. Each month, the healthcare industry faces cyber attacks and with yet no effective security measures in place, there is little to be done to fend off attackers.

Until recently, cyber security was not a primary concern for most healthcare businesses. Cyber attacks seemed to be focused on more lucrative businesses, and the healthcare industry thought itself safe. By not keeping protective measures up to date, healthcare organizations left themselves open to exploitation by hackers. One of the biggest areas of vulnerability is in user identify and access.

As more and more healthcare businesses continue to grow, managing information presents a bigger challenge. Data is shared across departments and organizations with access given to both employed staff and those contracted out. Managing user access and ensuring that those with access are prioritizing security is a daunting task. Cyber security experts and teams have to take into account multiple accesses - on site, remote and mobile - appropriate authentication measures, and who is allowed access to what? Keeping information and data secure from those seeking to access it with malicious intent is a full time job.

In order to fight security breaches and reduce the risk of a successful attack, a major shift in thinking needs to occur. The mindset that healthcare businesses will forever be overlooked by hackers needs to go and the more proactive thought that it's just a matter of time, needs to be adopted. By thinking that a cyber security breach is inevitable, businesses will be more apt to take the steps necessary now to combat an attack. To successfully secure the business as best you can, try automating as much of the process as possible! Automation can handle the routine checks and maintenance, and will free up internet security teams for more important tasks such as employee education of best practices for internet safety.

Internet security and privacy need to go through a huge overhaul in the healthcare industry. In order to combat the increasing number of breaches healthcare businesses are facing, cyber security must become the priority and given the resources needed to protect sensitive information and data.

Contact us by June 30th, 2016 for a FREE CyberSecurity Audit so that we can help protect you from the threat of attacks. Email us at info@it-on-demand.com or call us at (212) 235-0260 for more information.

IT ONDEMAND
it-on-demand.com

Favorite Quote of the Month:

"I've missed more than 9000 shots in my career. I've lost almost 300 games. Twenty-six times I've been trusted to take the game winning shot and missed. I've failed over and over and over again in my life. And that is why I succeed."

- Michael Jordan