What Hackers Don't Want You to Know About Securing IT in Your Business

Data security is becoming a much bigger issue as more people than ever have access to sensitive data and use it in their daily work. Add in an increasingly mobile workforce and safeguarding security and confidentiality becomes a major issue. The boundary between work IT and personal IT is blurring as people use laptops and tablets at work and at home to access data and perform their duties.

As increasing numbers of businesses use new technologies such as cloud computing and mobile devices and apps, the risk of hackers accessing money, financial information and sensitive business data becomes more real. The House Committee on Small Business addressed this issue recently during a special hearing called, "Protecting Small Businesses against Emerging and Complex Cyber-Attacks."

"Small businesses generally have fewer resources available to monitor and combat cyber threats, making them easy targets for expert criminals," said Chris Collins, chairman of the House Subcommittee on Health and Technology. "In addition, many of these firms have a false sense of security and believe they are immune from a possible cyber-attack."

The committee heard testimony from a number of technology professionals from the tech industry on cyber security and the impact a breach of security can have on a business. From business down time to literally millions of dollars, companies cannot afford to cast a blind eye to this issue. Here are

> "Security is, I would say, our top priority because for all the exciting things you will be able to do with computers - organizing your lives, staying in touch with people, being creative - if we don't solve these security problems, then people will hold back."
>
> - Bill Gates

RBF Services:

Accounting and Auditing

Tax Services

Management Consulting Services

- Accounting Systems
- Business Acquisitions
- Business Startups
- Business Process Improvement
- Financing
- General Business Counsel
- Succession Planning
- QuickBooks

Personal Financial Counseling

Industry Experience:

AgriBusiness Services

- Egg Processors
- Farming Operations
- Fertilizer Producers
- Food Processors
- Silo Manufacturers

Construction Industry Services

- Aluminum and Glass Contractors
- Bridge Contractors
- Building Supply Companies
- Commercial Building Contractors
- Drywall Contractors
- Landscaping Contractors
- Masonry Contractors
- Mechanical Contractors
- Plumbing Contractors
- Residential Building Contractors
- Steel and Iron Fabricators

Healthcare Services

- Assisted-Living Facilities
- Continuing Care Retirement Communities
- Healthcare Foundations
- Home Care Nursing Associations
- Hospital Authority
- Individual & Group Medical Practices
- Medical Billing Services
- Nursing & Rehabilitation Centers
- Personal Care Facilities
- Pharmaceutical Distributors
- Pharmacies
- Sub-acute Facilities

Manufacturing Industry

- Tool and Die
- Fabricators
- Mold Extrusions
- Snack Food
- Packaging
- Aluminum Siding
- Glass and Glazing
- Industrial and Automotive Tools

three security tips that were offered as part of the testimony:

1.) Your Data Has Left the Building

When it comes to cyber security, one of the biggest problems is the lack of education among owners and their employees, Collins said.

It is an overall recommendation by the House Committee and IT professionals that business owners and their IT departments need to stay up-to-date on issues relating to cyber security threats and should create a written security policy for employees. A company should determine whether employees are allowed to have personal data on business devices. Conversely, figure out whether business data should be permitted on their personal devices and what to do in case a device is lost or stolen. Employees may be transporting data on a USB device and not remember to take it off of a home computer after they have downloaded it on their own computer.

> "Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months."
> – Clifford Stoll

Share the document with employees and make certain that they understand what to do and why cyber security is vital. In addition, we recommend that the policy be reviewed with new employees and on a regular basis with all employees.

2.) Your Data is Not Protected

Protect the data contained within your IT systems with encryption. Most operating systems come standard with disk encryption, including BitLocker for Windows PCs and FileVault for Macs. These programs essentially convert the data on your systems into unreadable code that isn't easily deciphered by hackers.

3.) You Have Gone to the Cloud

Major capital investment is saved by going to the Cloud. Cloud computing is based on a collection of IT facilities, software, applications, platforms, servers and data storage. Because these are all connected by the Internet and their physical location is not important, they are said to be "in the cloud."

The IT security issue that the Cloud presents, though, is that your Cloud platform can be hacked, as well. It should be part of your vetting system to see what security methods your provider has in place. For example, many businesses use QuickBooks on the Cloud, PayPal as

JEFF BLEACHER

"For starters with IT security, use common sense. Don't open questionable emails or download from sites you don't know. Practice "safe computing." From a more strategic level, it's important for the organization to brainstorm on internal and external risks to the security of your data and to address those risks accordingly. From that risk assessment prepare an IT security plan and a social media policy. A further step would be to create a disaster recovery plan. Never skimp on security or IT staffing. It's too important a function for sound operations in your company."

KEN FALK

"There are two types of companies, those that know that they've been hacked and have done the appropriate damage control and those that do not know that they have been hacked. It's not a question of if you will be hacked, but when and having the current systems of damage control in place." That's not an original quote from me, but I think it sums up the issue of IT security quite succinctly."

What Hackers Don't Want You to Know About Securing IT in Your Business

a payment method and many other platforms where your data is used and stored and may be vulnerable should these platforms get hacked.

Social Media is also vulnerable as we witnessed several weeks ago when Twitter was hacked and posted a message about the White House having been invaded and President Obama being taken. The stock market reacted immediately with a 300 point drop, but quickly recovered when Twitter announced they had been hacked. Twitter has since beefed up its IT security in order to ward off any such incidents in the future.

> "Computers are magnificent tools for the realization of our dreams, but no machine can replace the human spark of spirit, compassion, love, and understanding."
>
> – Louis Gerstner

In Summary:

Protecting IT should be part of an ongoing strategy as we move toward extended uses of the Internet, the Cloud and Software as a Service (SAAS). IT expenditures will move beyond seeking efficiency gains through automation and streamlining processes, toward using technology to differentiate themselves from their competitors. Using data to create information assets for the business will give them insight into operations and customers.

While hacking scenarios continue to make the headlines, businesses can create the strategy for protection. Research shows that over 50% of security breaches are a result of end-user error, oversight, and ignorance, so starting with your employees by training them on IT security is an effective method of reducing end-user related security breaches.

LARRY REICH

"While I'm not the best IT person here at the firm, we all understand the value of investing in the front edge of technology. Companies that are well-invested in technology; hardware, software and staff – tend to be more profitable companies. So, from a strategic level, we make those investments. When it comes to me personally, I call the IT department. They are my "go-to guys!"

PATRICK GENDRUE (on the left)

"IT security is a critical issue for us and for anyone handling sensitive and confidential data. So, we've made it a priority to invest heavily in securing our data and records. We also find it's important to educate employees on securing data on a regular basis, especially now that everyone is so mobile with a wide variety of devices. Investment and education are key."

Disclaimer of Liability: Our firm provides this information for general guidance only, and does not constitute the provision of legal advice, tax advice, accounting services, investment advice, or professional consulting of any kind. The information provided herein should not be used as a substitute for consultation with professional tax, accounting, legal, or other competent advisers. Before making any decision or taking any action, you should consult a professional adviser who has been provided with all pertinent facts relevant to your particular situation. Tax articles are not intended to be used, and cannot be used by any taxpayer, for the purpose of avoiding accuracy-related penalties that may be imposed on the taxpayer. The information is provided "as is," with no assurance or guarantee of completeness, accuracy, or timeliness of the information, and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability, and fitness for a particular purpose.

Ross Buehler Falk & Company, LLP
Certified Public Accountants

1500 Lititz Pike
Lancaster, PA 17601

717-393-2700
717-393-1743 (fax)

www.rbfco.com

RBF is a Lancaster, PA CPA and consulting firm specializing in providing accounting and consulting services with the highest integrity.

Seven Tips for Work IT Security

Research shows that over 50% of security breaches are a result of end-user error, oversight and ignorance; so training your employees to follow processes and protocol is the place to start.

1.) Working with the IT Department: Install all of the patches and updates that your IT department asks you to do. There are continually updates that need to be installed for Windows and Office programs as well as security software to protect your individual computer. In addition, if you have a remote session through your server you want to make sure that your home computer has a firewall or security installed to protect you in remote locations. Making these regular updates will keep your computer and your company's network as secure as possible.

2.) Don't Use the Save Password Option: It's easy to hit "Remember Me on This Computer" but you should make it mandatory to enter your password on all operating systems or application settings. This will protect your computer from someone else easily accessing your data. And, remember to use a variety of passwords on all of your logins. It's easy to use the same one, but that makes it easy for anyone to figure out how to access your information; whether personal or data from the organization.

3.) Never Open Questionable Emails: Hackers and virus perpetrators have become very sophisticated at tricking people into opening innocent or official looking emails. If anything looks fishy at all, don't open it. Send it to your IT department so they can check it out and then alert everyone in the company about the potential danger. And never open anything that looks suspect regarding financial information. You should never be asked for your Social Security number from any source.

4.) Install only Licensed Software: Your company should have a license for all software installed on your computer. Unlicensed software can create legal problems so don't install software that's been given to you by someone other than your IT department. Additionally, software that's been purchased for home use may not be compatible with what's on your work computer and may cause problems down the line with upgrades and other applications.

5.) Don't Rely on Your Expertise: Many times employees try to fix things themselves and end up creating bigger problems for their computer as well as the network. It's best to ask your IT department immediately rather than hoping something will clear up on its own. Typically things will just get worse, especially if you have a virus on your desktop from that email you weren't supposed to open!

6.) Don't Download Programs from Sites You Don't Know: Downloading programs from sites you don't know may jeopardize the entire network. It may seem innocent enough to download a harmless app or program, but you should remember that your work computer is not your personal device and should only be used for work related activities.

7.) When in Doubt, Ask: Things are happening so fast in the IT world that you may not have the most current information about a program. Ask your IT Department whenever things may seem questionable. It's better to give IT the opportunity to research and evaluate an option then to risk taking your entire network down.

Change your passwords on a regular basis to ensure security for your company and your personal identity.

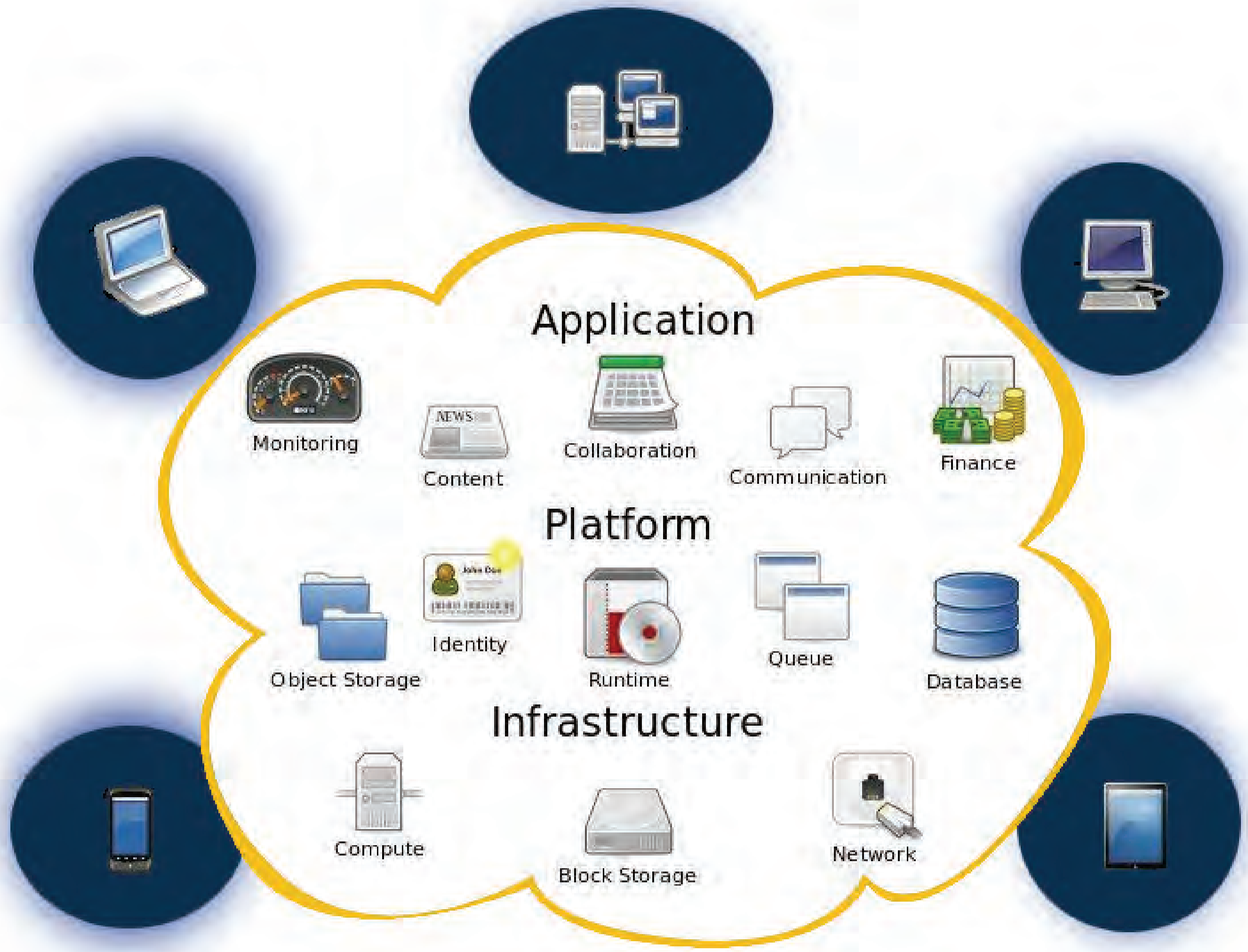
Disclaimer

Welcome to the Cloud!

Cloud Computing is an expression that has gained much popularity in recent years, and even though more than 50% of all businesses report using cloud computing, most people don't know what it means. Here is an easy way to "wrap your head" around the concept of "going to the cloud."

In technical terms, the cloud is a large network of servers that are connected, in real-time, typically through the Internet. This network of servers and computers allows for the ability of the software programs and applications to run simultaneously while multiple users can access the programs through a wide variety of devices. Since the programs and applications are housed on these networks, upgrades are available immediately to all users. The benefits of "going to the cloud" are numerous, but most significant is the economic benefit of subscribing to the software or application used – paying as you go – and the ability to share resources easily and efficiently.

The diagram below, courtesy of Wikipedia, shows the components of cloud computing and the ability of all devices to access the cloud from any location.


Application
Monitoring
Content
Collaboration
Communication
Finance
Platform
Identity
Object Storage
Runtime
Queue
Database
Infrastructure
Compute
Block Storage
Network