ITMS LLC

Is Your Information Safe From Prying Eyes?
Cyber Crime Happens All the Time

Hackers Are Always On The Prowl For Your Information
We are All Connected All the Time Through the Internet

All Business And Homes Have Data Connections That Can Be Exploited.
Anyone in the World Has Access.

An Attack Can Come From Anywhere. Nextdoor, A Car Parked Down The Street, Or The Other Side Of The World.
<table>
<thead>
<tr>
<th>Why be Concerned?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Data Loss</td>
</tr>
<tr>
<td>Personal Information</td>
</tr>
<tr>
<td>Intellectual Property</td>
</tr>
<tr>
<td>Company Reputation</td>
</tr>
<tr>
<td>Reputation</td>
</tr>
<tr>
<td>Heavy Fines</td>
</tr>
<tr>
<td>Legal Fees</td>
</tr>
</tbody>
</table>
How Strong are You?

Where Is The Weak Link?

How Do You Know?
Points of Entry

Email Social Engineering/ Spear Phishing

Infection via a Drive-By Web Download

USB Key Malware

Scanning Networks for Vulnerabilities and Exploitation

Wi-Fi Compromises

Exploiting Password Reset Services to Hijack Accounts
What do They Want

Your Data

Your Client’s Data

Credit Information

Medical Records
Insuranc Journal-
Worth 10 times more than CC

BOTS

Easy Money
The **S** in IoT

Stands for Security.

The **P** is for Privacy.
Should I Use Them or Not?

- Easy to Use
- Simple Setup
- Can be Helpful
- Productivity Gains
- Cost Savings
- Built for Ease of Use
Should I Use Them or Not?

Do you really need a lightbulb, camera, or whatever connected to the internet?

Change the default username and password.

Make the password a strong one.

Do not buy used IoT devices. This still may not help. **Best Buy**

Create a subnet for the IoT devices to be segregated from production.

Must you have a device listening all the time? It’s not! **Are you sure??**

Shut down inbound and outbound connections.

These Devices are Computers with an OS.

Not Built for Security
Two hackers appear to have created a new powerful zombie army. Bot

Solar array management device from Tigro Energy.

Trojan within a target's network to spy on it.

Used ASL-01 lock

Data collected by the Echo may be evidence in a case.

Police got data a smart water meter.

A smart fridge could be exploited so that an attacker obtains user credentials.
Mirai

Click Fraud
DDoS
Minecraft
500,000
Default
Passwords
Reaper

DDoS??

Security Flaws
Buy or Rent?

Prices range from $0.25 to $1 per host, with minimum orders of around 50-100.

100,000 units cost $7,500.
Cryptocurrency

Bitcoin
Ether
Litecoin
Monero
Dogecoin
How does it work?

Blockchain

Mining

Wallets

Anonymity
Cryptocurrency Crime

A Russian man, was, blindfolded, until he logged onto his computer and transferred about $100,000 worth of Bitcoin to an online wallet they controlled.

In New York City, a man was held captive by a friend until he transferred over $1.8 million worth of Ether.

A Turkish businessman was forced to hand over the passwords to his virtual currency wallets containing nearly $3 million worth of Bitcoin.
Cryptocurrency Crime

Crypto-mining malware is draining enterprises’ CPU power with an estimated 23% of organizations globally being affected by the Coinhive variant during January 2018.
The Next Attacks

Cell Phone

Medical Equipment
Information Week-
Death By Hacking: Tomorrow’s IT Worry?

Appliances
Where to Start

Policies

Computer Usage
Data Security
Password Controls
Physical Computer Room Security
Termination of Access
Data Backup
Change Control
BC Plan
Patch Mgmt. Policy

Workforce Training
What Can You Do

Scan From The Internet And Look For Holes In Your Defenses.
Pass the Defenses

What Happens If An Intruder Breaches The Wall?
Compliance Requirements

HIPAA
SOX
PCI
FRB
SEC
$2.25 million - CVS Pharmacy
Individuals affected: NA – A OCR investigation, launched in response to media reports on the topic, found several CVS pharmacies were disposing of protected health information in public dumpsters.

$1.7 million - Alaska Department of Health and Human Services
Individuals affected: 501 – An unencrypted USB hard drive containing patient information was stolen from a DHSS employee's car.

Adult & Pediatric Dermatology, P.C.
Has agreed to settle potential violations of the HIPAA, agreeing to a $150,000 payment. This case marks the first settlement with a covered entity for not having policies and procedures in place to address the breach notification.

The Hospice of North Idaho
will pay the US Department of Health and Human Services (HHS) a $50,000 fine in the first settlement to take place over a breach of protected health information that affected fewer than 500 individuals.
Overlooking risks leads to breach, $400,000 settlement

MCPN provides primary medical care, dental care, pharmacies, social work, and behavioral health care services throughout the greater Denver, Colorado metropolitan area to approximately 43,000 patients per year, a large majority of whom have incomes at or below the poverty level.

MCPN filed a breach report with OCR indicating that a hacker accessed employees' email accounts and obtained 3,200 individuals' ePHI through a phishing incident. OCR’s investigation revealed that MCPN took necessary corrective action related to the phishing incident; however, the investigation also revealed that MCPN failed to conduct a risk analysis. Prior to the breach incident, MCPN had not conducted a risk analysis to assess the risks and vulnerabilities in its ePHI environment, and, consequently, had not implemented any corresponding risk management plans to address the risks and vulnerabilities identified in a risk analysis.
I am Too Small

Why Worry?

THE HOME DEPOT

TARGET

ebay

SONY

J.P. Morgan
Big Leagues

Where Did They Start??
Cyber-Insurance??

We have no worries.
We're Insured.
What are the Terms?
Are You Sure?
Phishing Attacks

Ransomware.

Malware.

Espn_com@outlook.com

http://captureone.dx.am/capture.php?id=20

Breaking News!!

Super Star quarterback Payton Manning has been involved in a horrific multi car crash. News is updating quickly as to his condition. For the up-to-date information check our site.

www.espn.com/payton/crash
Demo
<table>
<thead>
<tr>
<th>Severity</th>
<th>Plugin Id</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical (10.0)</td>
<td>10380</td>
<td>rsh Unauthenticated Access (via finger Information)</td>
</tr>
<tr>
<td>Critical (10.0)</td>
<td>25216</td>
<td>Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow</td>
</tr>
<tr>
<td>Critical (10.0)</td>
<td>32314</td>
<td>Debian OpenSSH/OpenSSL Package Random Number Generator Weakness</td>
</tr>
<tr>
<td>Critical (10.0)</td>
<td>33850</td>
<td>Unsupported Unix Operating System</td>
</tr>
<tr>
<td>Critical (10.0)</td>
<td>34970</td>
<td>Apache Tomcat Manager Common Administrative Credentials</td>
</tr>
<tr>
<td>Critical (10.0)</td>
<td>46882</td>
<td>UnrealIRCd Backdoor Detection</td>
</tr>
<tr>
<td>Critical (10.0)</td>
<td>51988</td>
<td>Rogue Shell Backdoor Detection</td>
</tr>
</tbody>
</table>
### 25216 - Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>It is possible to execute code on the remote host through Samba.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>The version of the Samba server installed on the remote host is affected by multiple heap overflow vulnerabilities, which can be exploited remotely to execute code with the privileges of the Samba daemon.</td>
</tr>
<tr>
<td><strong>See Also</strong></td>
<td><a href="http://www.samba.org/samba/security/CVE-2007-2446.html">http://www.samba.org/samba/security/CVE-2007-2446.html</a></td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>Upgrade to Samba version 3.0.25 or later.</td>
</tr>
</tbody>
</table>
Questions?
WASHINGTON — If you’ve been remiss in cleaning out your email in-box, here’s some incentive: The federal government can read any emails that are more than six months old without a warrant.

Little known to most Americans, ambiguous language in a communications law passed in 1986 extends Fourth Amendment protections against unreasonable search and seizure only to electronic communications sent or received fewer than 180 days ago.

The language, known as the “180-day rule,” allows government officials to treat any emails, text messages or documents stored on remote servers — popularly known as the cloud — as “abandoned” and therefore accessible using administrative subpoena power, a tactic that critics say circumvents due process.

As you rush to purge your Gmail and Dropbox accounts, however, be forewarned that even deleted files still could be fair game as long as copies exist on a third-party server somewhere.

Bipartisan legislation introduced earlier this month would require government agencies and law enforcement officials to obtain a search warrant based on probable cause to search the public’s emails that are 180 days old and beyond.

CHERYL DIAZ MEYER — McClatchy