HACKERS, CRACKERS, BOTS, MALWARE AND WEB 2.0
DATA SECURITY CHALLENGES IN THE ALL TOO PUBLIC AND NOT SO PRIVATE SECTORS
I want you to take home four points

- Understand
- Educate
- Collaborate
- Prepare
It’s a great to be in Blue Ash today, but uh, do you know where your data is right now?

- The confidentiality
- The integrity
- The availability
- It’s hard to protect that which we have no idea as to its whereabouts
So, where is your data today?

- On any device
- Any place
- Any time
- When “aren’t” we working anymore?
- When do we call it a day?
- We don’t, do we?
Today, it’s about mobility...

- In the past few years we shifted our lives to the PC and the Internet
- Now, it’s all about being mobile
- A PC in your pocket
- Our mobile work force is growing and expanding
Where?

- Where does work happen?
- No longer does business take place solely behind network walls
- The critical work is happening increasingly on social networks, on handheld devices, in the field, and at local cafes
Diminishing Border

- The traditional corporate perimeter, with clearly identifiable boundaries, has diminished
- In its place, a network with limitless potential is rising
- One where agencies, companies, their customers, and their partners demand access to information whenever and wherever they need it
New Considerations

- It is information technology’s role to ensure that the appropriate people, using the correct devices, are accessing the proper resources while having a highly secure yet positive user experience within your networks.
New Considerations

- Operations, behaviors, and ideas are transcending the artificial boundary outside of the network perimeter—the firewall—and, in turn, are being shared in ways that current security models may not have considered
A blurring of activities

- In addition, it is common for workers to blend business and personal communications on these social networks, further blurring the network perimeter
Cisco Study Finds Telecommuting Significantly Increases Employee Productivity, Work-Life Flexibility and Job Satisfaction

Increased Productivity Due to Telecommuting Generates an Estimated $277 Million in Annual Savings for Company

SAN JOSE, Calif., June 25, 2009 – Today, Cisco announced the findings of its Teleworker Survey, an in-depth study of almost 2,000 company employees. The study, conducted to evaluate the social, economic and environmental impacts associated with telecommuting at Cisco, revealed that a majority of respondents experienced a significant increase in work-life flexibility, productivity and overall satisfaction as a result of their ability to work remotely.

As the modern workforce continues to evolve and globalize, more companies are evaluating a telecommuting strategy to save costs and lower carbon emissions as well as to retain top talent. For these companies, Cisco’s survey highlights the gains that a sound telecommuting strategy provides for employees and employers alike.
Our own technologies
Remember when...

- Security meant having someone who could set a rule on a firewall
- The security officer was the guy at the desk in the lobby
- Browsing was something you did at a Mall
- Podcasting was throwing peas into the wind
Remember when...

- Intrusion prevention was locking your front door
- Identity theft was handing in someone else’s homework
- Data loss was forgetting where you put your car keys
- Those days are gone...
Where are we going and what are we doing?
Facebook

- Over half a billion users
If Facebook were its own country, it would be the third most populous nation in the world behind China and India--both countries have populations north of one billion people.
Some bone-jarring statistics

- 50% of Facebook active users log on to Facebook on any given day
- More than 60 million users update their status daily
- People spend over 500 billion minutes per month on Facebook
Billions

- More than 3 billion photos uploaded to the site each month
- More than 5 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each week
The involvement is viral

- Millions of local businesses have active Pages on Facebook
- More than 20 million people become fans of Pages each day
- Pages have created more than 5.3 billion fans
Mobility

- There are more than 100 million active users currently accessing Facebook through their mobile devices.
Cisco on Facebook

Cisco

We're only one day away from the Enterprise Cisco Collaboration TweetChat. Join our panel of experts on Twitter as they discuss enterprise policy, unified content models, and interoperability all in relation to Enterprise Collaboration


yesterday at 6:40pm · Comment · Like · Share

46 people like this.

View all 6 comments

Maryam Mohsenzadeh loves this. 2 hours ago · Flag

Buti Mokhe: love Cisco too. 2 hours ago · Flag

Write a comment...

Comment

Cisco Robert Pepper is taking your questions NOW about the global demand for broadband. He'll discuss how it is growing everywhere and how it is driven by video.

Talk2Cisco: Global Demand for Broadband

share:

Atlanta Bucket List

Things to do in Atlanta before you die. One hope coupon emailed daily.

Like

AARP® Medicare Supplement Insurance plans issued by United Healthcare Insurance Company. Request a Free Information Kit today.

Like

Expressive Signs & Designs

Located in Alpharetta, we provide all types of interior, exterior or vehicle signage. Click this link button to become a fan.

Like

Move Ads
Cisco Wikis

The Cisco Learning Network

Connections

Team Wiki Spaces

Overview All Content Discussions Documents

TEAM WIKI SPACES

Collaboration is key.

If your technology group needs a place to share ideas and coordinate concepts, a Team Wiki Space on the Cisco Learning Network might be just what you need. You can email us to request information on your own Team Wiki Space. We are currently evaluating teams for inclusion in this cutting-edge environment.

Current Private Team Wiki Spaces

There are no sub-communities.

Keep on Keepin' on!

Modern work is collaborative, where many people work hard and move at a fast pace. Interaction is key.
Shop 'Til You Drop: Either from Exhaustion or Poor Connectivity

I'm a shopper. I'll admit it. I love the thrill of the hunt and the eventual bagging of a fun or exotic item that plays to my fashion sense or inner tech geek. So, as someone who straddles the worlds of technology and retail, I can't help noticing the spate of articles and information lately on how interlinked social media and shopping are becoming. And how the borderless experience I've talked about in the past several months is becoming more and more critical for businesses to enable.

This week, a New York Times article reported comScore's latest overview of the online retail economy. According to the report, the more time users spend at social media sites, the more money they spend online. For instance, heavy users of one of the most popular social media sites, Facebook, spend an average of $57 versus “light” network users who spend $30, on average, or non-users of the network who only spend an average of $27 online.

Read More.

Posted by Marie Hettar at 11:55AM PST

---

Australian, New Zealand & Chinese Students Go To Class Across Asia - Without Leaving their Seats

---
Cisco on Twitter
Cisco on YouTube
What else are they doing?

- In August, people spent a total of 41.1 million minutes on Facebook
Facebook outage spotlights social media addiction

- After Facebook went down on Thursday, one thing was certain: People don't like to go without their favorite social networking site.
- Industry watchers say Facebook users suffering through the two-and-a-half-hour outage were like drug addicts going through withdrawal.
In despair...

- Facebook's more than 500 million users have grown accustomed to sharing updates about their cats and colleagues, and posting funny pictures of drunken friends and kids acting silly.
OWASP on Twitter
On Facebook
Overall, 43 percent of Americans said they keep in touch via social networking websites such as Facebook, MySpace and LinkedIn.

Forty percent of men, and 45 percent of women, said they had a profile on a networking site.
There is a human element to all of this, an element that is more often than not, overlooked...
It’s no longer just close relationships

- Our employees are going places they’ve never gone before and are touching technology daily
- That which they are touching is touching our networks as well
Web 2.0?

- Businesses today find that social media use is no longer the exception, but rather the rule.
- It marks the global trend of seeking friendships or relationships online.
Who is using it?

- Business units such as research and development, marketing, human resources, sales, and customer service
- They are realizing the potential for utilizing social media tools to stimulate innovation, create brand recognition, hire and retain employees, generate revenue, and improve customer satisfaction
With Web 2.0

- A new breed of malware is evolving
- Google Mashups, RSS feeds, search, all of these can be misused by hackers to distribute malware, attack Web surfers and communicate with botnets
Risk – it's everywhere

- And no one knows that better than IT security professionals
- Disgruntled employees, students, fired employees, clueless employees who succumb to social engineering, passwords left on Post-it notes, wide-open instant messaging and increasingly powerful hacker tools in the hands of teenagers, Web Mobs and Organized Crime targeting Social Media sites
Objective?

- The key objective, of course, is to recognize risk, safeguard your reputation and not reveal sensitive or confidential information that may prove harmful to your business
Social Media Benefits

- It is very difficult to argue with many of the benefits being provided by the numerous social media networks for both personal and business purposes.
Information sharing

- These networks, Facebook, Twitter, LinkedIn, and YouTube to name some of the heavy hitters, enable millions of people to exchange up-to-the-minute information with each other across the globe.
Concerns

- As with most new voice, video, and data applications that traverse the network, this pervasiveness brings with it additional security concerns.
How do we secure it?

- It becomes difficult and, in fact, almost contradictory for organizations to crack down on the use of social networks while they are simultaneously promoting the use of such networks to do business.
Ease the burden

- This balancing act can be made a bit easier through:
  - The development and enforcement of corporate security policies
  - Ongoing education of employees in the proper use of social networks when corporate assets are involved
  - The identification and mitigation of related malware using network and host-based anomaly detection technologies
Malware

- Historically, malware has plagued e-mail, hidden in malicious attachments

- While that's still happening, more malware writers are putting their efforts into malicious Web sites
Constant Mutation

- The goal in developing malware is not to simply infect as many systems as possible but to specifically steal usage information and other data from compromised systems.
- Use of polymorphic code that constantly mutates.
Bad Statistic

- 1 in 1,000 web pages is infected with malicious drive-by download software
Two biggest vectors for Malware

- Email
- Web-based
So, what do we have to do?

- Create a Human Firewall
The Human Firewall – an invaluable tool

- A good *human firewall employee* is one who filters good security practices and rejects any others—much like a network firewall only allows authorized traffic and rejects any other.
- The only way to build a good human firewall is to raise people’s awareness; to teach them good habits, to make them recognize bad practices and change them into good practices.
- Your cyber security is only as good as the people who manage it and those who use it.
So Patrick, why do we really need that Human Firewall?

- Because, ‘Friend’ has become a verb
- Social media users believe there is protection in being part of a community of people they know
- Criminals are happy to prove this notion wrong
- The threats and security issues that come with social media aren’t usually caused by vulnerabilities in software
- More commonly, these threats originate from individuals who place an unwarranted amount of “transitive trust” in the safety of these communities
Remember...

- On social sites –
  - Your privacy is history
  - They don't have your best interests in mind
  - Social engineering attacks are getting more targeted
Trust?

- Users will trust something or someone because a user they know has also expressed trust in that person or subject
- We trust because we are curious and curiosity...
Curious? This is why! Out of date???
Or a Big Mac!
They want to send us somewhere else...

---

From: Automated Clearing House (ACH) [mailto:********@nacha.org]
To: ********@********.com
Subject: Unauthorized ACH Transaction Report

Dear bank account holder,

The ACH transaction, recently initiated from your bank account (by you or any third party), was rejected by the Electronic Payments Association. Please review the transaction report by clicking the link below:

[Unauthorized ACH Transaction Report]

Copyright ©2009 by NACHA - The Electronic Payments Association
The unknown... DO NOT TOUCH THIS!!!

XP antivirus Online Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Risk level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware.IEMonster.b</td>
<td>Spyware</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>Zlob.PornAdviser.Xplisit</td>
<td>Spyware</td>
<td>High</td>
</tr>
<tr>
<td>Trojan.InfoStealer.Banker.s</td>
<td>Trojan</td>
<td>Medium</td>
</tr>
</tbody>
</table>

[Remove All] [Ignore]
## System Scan

**Scan & fix your computer**

### Scan type:
- Quick
- Deep
- Memory Scan

### Scan Results

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Type</th>
<th>Location</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan-Cookie.Win32</td>
<td>Malware</td>
<td>C:\Documents and Settings\Hoai_K...</td>
<td>Medium</td>
</tr>
<tr>
<td>GayCodec.lookAlert</td>
<td>Malware</td>
<td>C:\WINDOWS\System32\yeshatm.dll</td>
<td>Medium</td>
</tr>
<tr>
<td>webSearch.Win32</td>
<td>Malware</td>
<td>C:\WINDOWS\System32\Drivers\s...</td>
<td>Medium</td>
</tr>
<tr>
<td>PORN.perversion.R30</td>
<td>Malware</td>
<td>C:\WINDOWS\System32\Drivers\s...</td>
<td>Medium</td>
</tr>
<tr>
<td>Virus.Win32.Gpc0</td>
<td>Viruses</td>
<td>C:\WINDOWS\System32\Drivers\Wbe...</td>
<td>High</td>
</tr>
<tr>
<td>Email-Worm.Win32</td>
<td>Network</td>
<td>C:\WINDOWS\System32\Drivers\s...</td>
<td>High</td>
</tr>
<tr>
<td>Net-Worm.Win32</td>
<td>Network</td>
<td>C:\WINDOWS\Fonts\858855.png</td>
<td>High</td>
</tr>
<tr>
<td>Net-Worm.Win32</td>
<td>Network</td>
<td>C:\WINDOWS\Fonts\small.png</td>
<td>High</td>
</tr>
<tr>
<td>Trojan-Downloader</td>
<td>Trojan</td>
<td>C:\WINDOWS\Help\camera.png</td>
<td>Medium</td>
</tr>
</tbody>
</table>

### Scan complete.
- Objects scanned: 30329
- Threats detected: 19
  - Removed: 0

### Upgrade to full version now!
- Easy one-click registration

**Your Computer is not protected**
- Click here to fix security problems
To help protect your computer, Windows Firewall has detected activity of harmful software.

Do you want to block this software from sending data over the Internet?

Name: **Trojan-Spy.Win32.GreenScreen**
Risk Level: **CRITICAL**
Description: This is a spy trojan that installs itself to the system, hides itself and then captures screen images and saves them to disk files in encrypted form. Thus it allows a hacker to watch screen images.

- Keep Blocking
- Unblock
- Enable Protection

Windows Firewall has detected unauthorized activity, but unfortunately it cannot help you to remove viruses, keyloggers and other spyware threats that steal your personal information from your computer, including your Credit Card data and access passwords to the online resources you use. [Click here to pick recommended software to resolve this issue.](#)
YOUR SYSTEM MAY BE INFECTED!

Scanning:

Internet threats and viruses found:

FREE SCAN NOW!
Social Media Policy, Guidelines

Cisco Social Media Guidelines, Policies and FAQ

We take social media seriously at Cisco.

We look at it as a collaborative tool to help better serve our customers, our partners, our investors and our employees... and to LISTEN to them as well. There, of course, have to be guidelines and employee training around the use of social media. Within our company culture of transparency, we thought we’d make our newly updated Internal Social Media handbook available for everyone. We don’t claim to know everything about Social Media, but we do know that the wisdom of the crowd is generally better than the wisdom of the few. With that in mind, we welcome your thoughts, observations and viewpoints on our Social Media Policy and Guidelines.

Cisco Social Media Guidelines - June 2010
But what does all this mean?

- I am just an employee and am not an engineer or a technician or a programmer or a geek!
- I’m just sitting at my desk, talking to friends, patients and all sorts of people
- How in the world am I threatening our network???
2 Reasons...

- You probably do not understand policies, procedures, best practices and standards.
- If you do understand them, they are violated because there are no consequences – the policies are not enforced.
- Who, me?
Education is Critical

- Few executives grasp the case for investing in safeguards against hackers, malware, and the like.
- Education starts at the top and works its way down the food chain throughout the entire business.
- Before any employee puts their fingers on the keyboard they must understand that it is not their computer.
The Seven Deadly Sins of Network Security

1. Not measuring risk
2. Thinking compliance equals security
3. Overlooking the people
4. Too much access for too many
5. Lax patching procedures
6. Lax logging, monitoring
7. Spurning the K.I.S.S.
You Must Understand...

- That you are a target
- These hackers are smart, and most have much more time to spend attacking them than a typical systems administrator can spend defending against them
The Opposing Team

- The Hackers
- Disgruntled Insiders
- Clueless employees
- Competitors
- Foreign Governments
- Terror organizations
Top 8 Perceived Threats

- System penetration
- Sabotage of data
- Theft of proprietary information
- Denial of service
- Viruses and Worms
- Unauthorized insider access
- Laptop theft
- Insider abuse of the Internet
System Penetration

- It is an unfortunate reality that you will suffer a breach of security at some point.
- To bypass security, an attacker only has to find one vulnerable system within the entire network.
- But to guarantee security, you have to make sure that 100 percent of your systems are invulnerable -- 100 percent of the time.
Data Leakage:
How many breaches in 2009?

- 498 Breaches
- 222,477,043 records exposed
- How were you impacted?
Who?

- Businesses - 36 percent
- Healthcare - 29.2 percent
- Government, military - 16.9 percent
- Financial Services – 11.1 percent
2010

- 327 Data Breaches
Not good...

- But Patrick! It won’t happen to us!
Whether you get hacked depends...

- Do you assume the posture of, “It can’t happen here.”
- Do you hear, “We haven’t heard of any worm outbreaks and all seems quiet. Why upgrade those devices?”
- “We have no budget.”
- “We’re just hanging out in Cincinnati!”
- “They’re only going after the Government and those really big banks.”
- Then my question is, “Can you really afford to give up data today?”
You can’t! So,

- Be compliant but don’t rest on your laurels
- Be vigilant
- Educate
- Know that you are a target
- Be ready to respond
So, what are they really after?

- Your Intellectual Property
- Your assets
- Your employee’s data
- Your personal data
- Your paycheck
- Your friends
- Your family
G-Man’s tips to secure your data

- **Consider threats** from insiders and business partners in your enterprise-wide risk assessments
- **Clearly document** and consistently enforce policies and controls
- **Institute periodic** security awareness training for all employees
G-Man’s tips to secure your data

- **Monitor and respond** to suspicious or disruptive behavior, beginning with the hiring process
- **Anticipate and manage** negative workplace issues
G-Man’s tips to secure your data

- Implement **strict** password and account management policies and practices
- Enforce **separation** of duties and least privilege
- Implement **system change** controls
- Log, monitor and audit employee online actions
- Use **layered defense** against remote attacks
G-Man’s tips to secure your data

- Deactivate computer access following termination
- Implement secure backup and recovery processes
- Develop an insider incident response plan
You are the last line of Defense! Don’t drop the ball!!!

- Understand
- Educate
- Collaborate
- Prepare
Thank You!

pagray@cisco.com