HOWARDTECH ADVISORS

Cyber Risks

(And What To Do About Them)

Ananta Hejeebu

April 15, 2015

Background

- Managing Partner for IT Services firm
- Client size 5-125 employees, many with multiple offices.
- Assume responsibility for all client technology issues. Shared risk.
- Technology is critical to many firms yet owners often can't (or won't) slow down to look at IT strategically.

Are We Secure?

Mon 12/22/2014 9:39 AM

Ananta Hejeebu

RE: security

To [redacted]

You forwarded this message on 12/22/2014 9:44 AM.

"Secure" is a relative word. [redacted] is very secure compared to most small businesses, yet a determined attacker would likely overwhelm the security infrastructure that's been put in place. We have deployed numerous best practices for you, but it would be inaccurate to say we are 100% secure.

Most security breaches today are not caused by hackers (outside attacks), though the Sony, Target, Home Depot, and other incidents get all the press. Rather, most are caused by employees (internal staff) - some deliberately (someone takes or shares company data) or accidental (someone clicks on a link that allows a virus on to the company network). Most viruses are annoying (popups, etc.) but criminals are using viruses to gain access to critical data, steal money, etc. This is a huge and is only solved by ongoing employee education, as a system can't stop a virus from getting in if a user explicitly allows it.

It would be wise to review with you or [redacted] or other the security protocols that are currently in place for [redacted] and our recommendations to further tighten things up. Maintaining a secure computer system is an ongoing process, so it would be ideal to review with you at least once per year or more depending on your concern level. Are you available to discuss?

The important point to make is that security and convenience are in constant conflict. The more secure I make something, then the less convenient it is for the users. If I want things to be more convenient, then it will be less secure. The proper balance between these two is a judgment call that each of our clients makes.

Bottom line is that [redacted] has a good system in place. Let me know if you want to review our recommendations to improve security.

From: [redacted]
Sent: Sunday, December 21, 2014 12:16 PM
To: 'Ananta Hejeebu'
Subject: security

Are we secure? Do want a Sony to happen.

Cyber Risks

- Targets – Large business vs. SMBs
- Sources – Internal vs. External
- Motivation – Accidental vs. Intentional
- What can I do to reduce risks?

Targets

- Large business
  - Lots of press attention
  - Varying goals – IP, money, publicity
  - Deception or large scale attack
  - Increasingly sophisticated schemes

- SMBs
  - Very little exposure, but likely more common
  - Seeking money, your or your customers'
  - Deception is common route
  - Increasingly sophisticated schemes

Sources & Motivation

- External
  - Makes sense (bad people in the world)
  - Goal is clear (do bad things)
  - Attacks are often not obvious
- Internal
  - Not my employees!
  - Motive may be intentional or accidental
  - Timing may coincide with certain events

A good security strategy will consider all factors, and be multi-layered. There is no key!

What Can I Do?

1. Document all data repositories

   - What information is stored where? (PCs, laptops, servers, cloud, USB stick, offsite, external hard drives)
   - Consolidate where possible
   - Restrict access only to those needing
   - How is each repository backed up? (Assume you will be attacked)
   - Develop a regular disaster recovery (DR) test schedule. Plan for disruptions.

What Can I Do?

2. Deploy Robust Security Tools

   - Business firewall – purpose built UTM device
     - Content filtering
     - Intrusion prevention
     - VPN for remote access
   - Windows and software updates
   - Anti-virus and anti-malware
   - Spam filtering
   - Maintenance utilities (Ccleaner, etc.)
   - Email encryption and archiving

What Can I Do?

3. Implement Security Best Practices

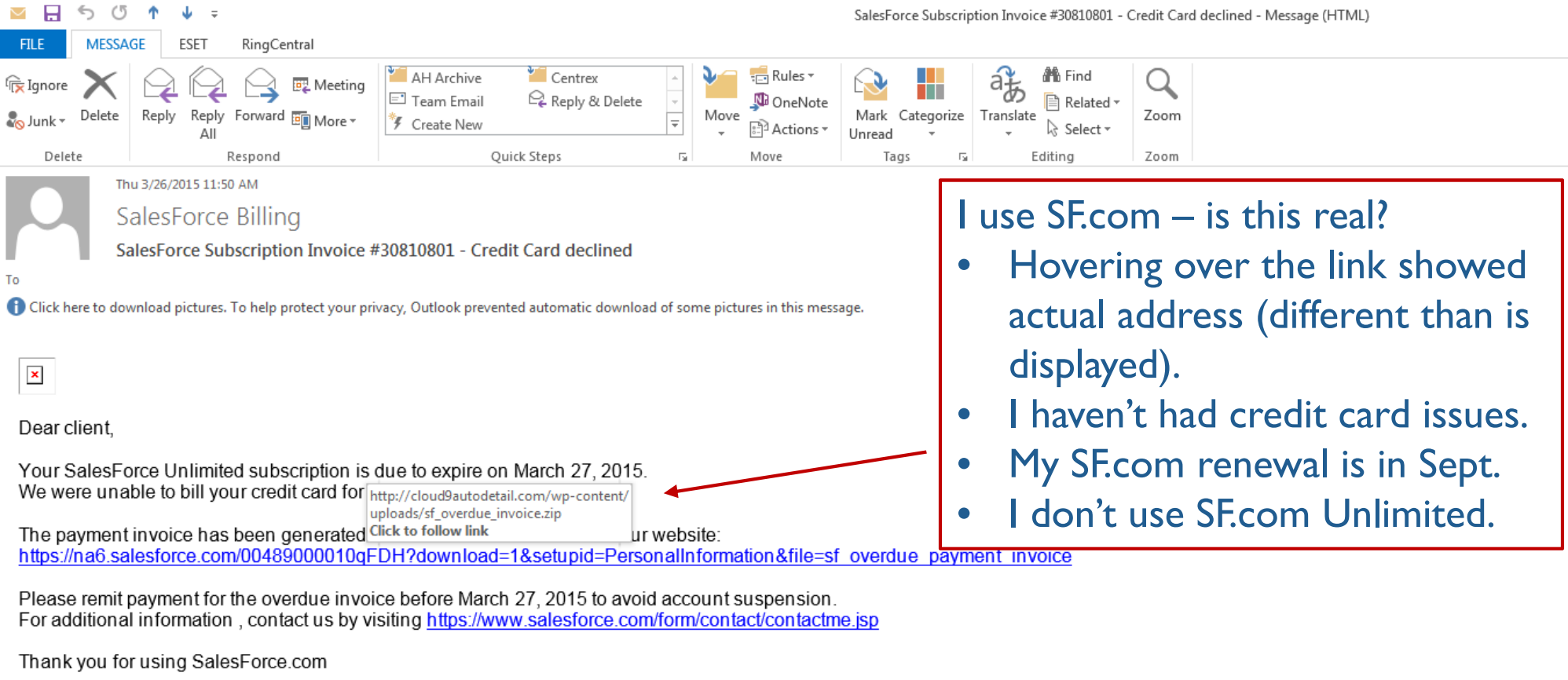
   - Password complexity/change policy
   - Separate your network into VLANs
   - Create a separate guest wireless
   - Use central authentication for wireless
   - Review (or develop) permissions for all folders and data repositories
   - Encrypt hard drives for laptops
   - Ensure phones/tablets can be wiped remotely
   - Run cleaning tools regularly
   - Do nothing private on a public network
   - Never save passwords in your browser

What Can I Do?

4. Employee Training (Constant)

   - Create a security-aware culture (what to trust, awareness, paranoia)
     - Banking Trojans
     - Ransomware
     - Keystroke logging
   - Email & Websites
     - Never click links in any email (go directly to sites – FB, LinkedIn, etc.)
     - Be vigilant and always skeptical (phishing)
     - Be cautious of opening any attachments
     - Don't accept friend requests from strangers or watch videos that seem suspicious

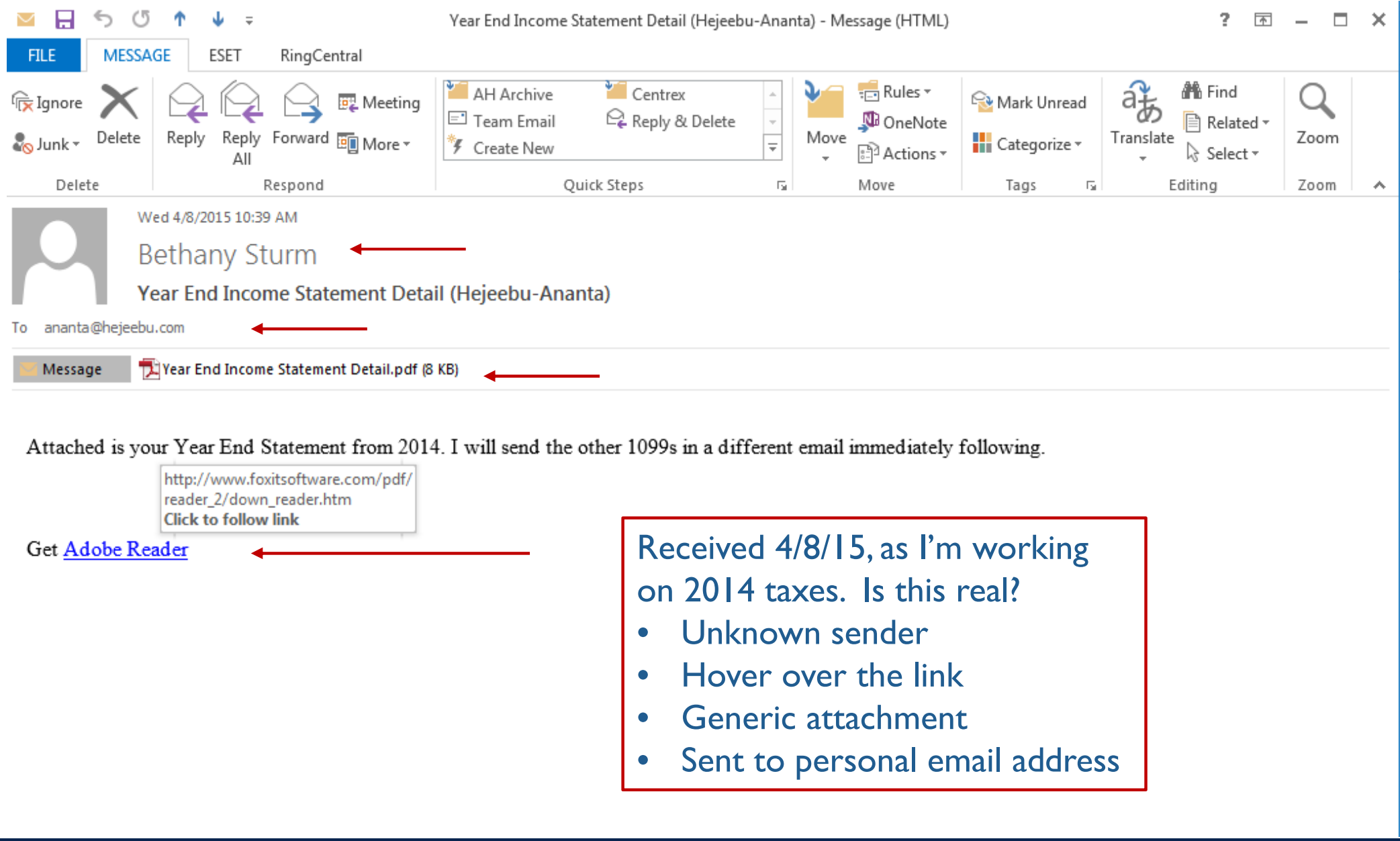
What Can I Do?



I use SF.com – is this real?

- Hovering over the link showed actual address (different than is displayed).
- I haven't had credit card issues.
- My SF.com renewal is in Sept.
- I don't use SF.com Unlimited.

What Can I Do?



Received 4/8/15, as I'm working on 2014 taxes. Is this real?

- Unknown sender
- Hover over the link
- Generic attachment
- Sent to personal email address

What Can I Do?

5. Other things to consider

- Use a dedicated PC for online banking
- Leverage 2 factor auth. for all cloud services
- BYOD – consider the risks associated
- Physical security – make your office tight
- Employee background checks – how to monitor for potential risks
- Automate updates, particularly OS and AV
- Restrict everything – mobile, wifi, webmail, content, files, access, etc. – possible
- Regularly review security and backup policies with your IT partner

Closing Thoughts

- Examples cited are most common, of course there are many others.
- Identify small things to fix – build momentum and tighten over time.
- Cyber threats are significant, and only growing.
- Security & Convenience are in constant conflict. Figure out a good balance and review regularly.