TMC's ADVISOR

Covering IT and Telecom from a Western Canadian Viewpoint — *February 2015*

It's All About People Issue

Just When You Thought You Were Safe—The Dangers of BYOD

By Peter Aggus

There are many advantages to allowing employees to connect their own devices to corporate networks. Employees like the convenience and it's an increasingly popular way of saving money on hardware purchase. Of course, Bring Your Own Device is not all positive. Here's a summary of the risks.

Read More

Inside

People Want to Listen When... - By Thomi Glover

Last month, Ellen described her surprise at the results of her Personal Styles Inventory. It was fun to help her learn how to increase her credibility with others. Since our 'style' naturally attracts some people and drives others away, it's important to learn to work well with anyone. Happily, this can be learned.

Data @ Large: The Real World of Data, Privacy and Security - By Ellen Koskinen-Dodgson

The 16th Annual Privacy & Security Conference was held this month at the Victoria Conference Centre. It was a great success with the primary message being that the world is scary, from a privacy and e-security point of view and it's getting scarier. From the introduction of Arpanet a scant 45 years ago to the internet that we know – things are much worse than I thought.</P>

The People Side of BYOD - By Ellen Koskinen-Dodgson

Most employees don't like corporate BYOD policies. They love the idea of BYOD but they resent the restrictions that come with it. Resentful employees cause major security risks but so do the everyday employees who are too trusting, who think that the sky will never fall. Here are some ways to improve employee behaviour.

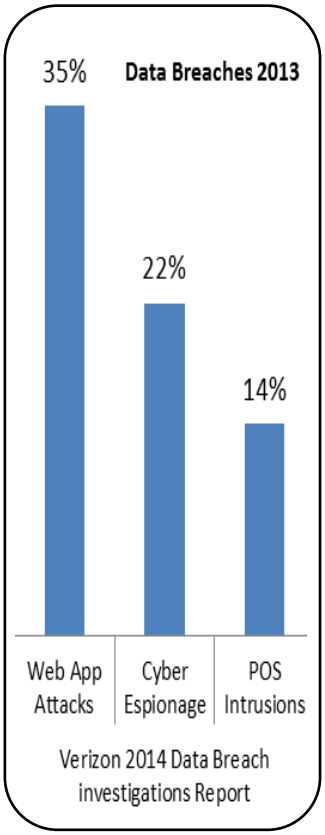
Penetration Testing

Attacks are everywhere and attacker sophistication is constantly increasing. Verizon's survey reported 63,000 security incidents and 1400 data breaches in 50 global companies.

The top three most common data breach techniques are:

- Web app attacks
- Cyber espionage
- POS Intrusions

TMC can perform an **external penetration test** of your network as well as a scan of your customer-facing web applications using a specialized security assessment application.



The Dangers of BYOD

By Peter Aggus

There are many advantages to allowing employees to connect their own devices to corporate networks. Employees like the convenience and it's an increasingly popular way of saving money on hardware purchase. Of course, Bring Your Own Device is not all positive. Here's a summary of the risks.

The Appeal

It started with senior managers wanting to connect their iPhones and iPads to the corporate network. Then it spread until most employees asked why they needed to carry a personal phone as well as a company phone. On the face of it—not a bad idea.

What's The Problem?

Any connection, by any mechanism, poses a risk to corporate security. Risk can be reduced but not eliminated. Organizations develop mobility strategies with associated policies, management technologies and procedures. The resulting security levels place organizations somewhere on the spectrum from not very secure at all to fairly tightly nailed-down. Except for the most highly nailed-down environments, many risks exist.

Exposure can include:

1. Device password is disabled or set to a simple value.
2. Device is lost or stolen. Risk continues until loss is reported.
3. Location tracking is disabled.
4. Encryption is disabled.
5. Device is 'shared' with family or friends so the user is unaware of unauthorized corporate access.
6. Remote data wipe is disabled.
7. User installed a rogue app.
8. User does not have mandatory corporate apps installed.
9. Device is not kept current with operating system, software and antivirus/antimalware updates.
10. User chooses to be a hobby hacker and has 'jailbroken' their device to bypass protective restrictions.
11. User uses Dropbox or other non-corporate file sharing services.
12. User updates documents locally and changes are not synced to corporate files.
13. Use of non-secure WiFi systems.
14. User connects via corporate WiFi while their cellular data connection is active, allowing unintentional pass-through access.
15. Authentication is weak.

What's the Cause?

With a limited number of IT-caused exceptions, the problem is human nature. Users are not naturally security conscious. In fact, people are generally security risk deniers, working on the basis that "nothing bad has ever happened before." Users expose their phones to theft by carrying them in their hands or leaving them on a restaurant table. They don't like the hassle of remembering and changing passwords. They want convenience. They don't like being tracked by geolocation. They want to use the cool new app. They're afraid to report a lost device as a remote wipe will mean the loss of personal photos and documents. They don't like the increased battery drain of some of the corporate security apps. The list goes on.

What's the Solution?

Of course, every organization needs to choose from the range and level of technology that best meets their needs.

However, it's much more important for every organization to focus on the people-side of mobile security (a topic we look at further in The People Side of BYOD).

This article is reproduced from the February 2015 edition of ***TMC's Advisor***

Peter, as an engineer and technology management consultant, has developed innovative and cost-effective solutions for clients in many industries.

People Want to Listen When...

By Thomi Glover

Last month, Ellen described her surprise at the results of her Personal Styles Inventory. It was fun to help her learn how to increase her credibility with others. Since our 'style' naturally attracts some people and drives others away, it's important to learn to work well with anyone. Happily, this can be learned.

It's All About Us

We all have our own preferences for how we use time, attend to tasks, relate to others, and express ourselves. Taken together, these preferences usually make us effective in some ways but less so in others. For example, highly task-oriented people are usually so focused on 'getting it done', that they may not notice how people around them react. So the hard-driving task person 'gets it done' but loses the support of the team, or worse, drives a client away. Conversely, highly self expressive people can be so busy talking, often about themselves, that the 'keep it brilliant and brief' task-focused colleague or potential client gets impatient and 'walks away.'

It's All About How Others See Us

We often don't see ourselves the way others do, and it's how they see us that makes them decide whether to listen to us, to trust us, to want to work with us and to do business with us. ***Our credibility with others is their perception, not our intention.***

We are often so wrong about how we think that others see us that we don't immediately agree with the results of our own assessment. One client was so skeptical that I suggested he share it with his wife....who apparently laughed aloud, saying she'd never seen such an accurate description of him. It's important to share assessment results with colleagues.

Knowledge is Power

Understanding how others see you and learning how to adjust your approach to work best with people with differing styles is the secret to the power of these techniques. When you learn to understand how to use the techniques, you can increase your personal credibility and make people want to listen. Your knowledge can even improve your team's performance.

In the old days, a manager tended to surround himself with clones of himself. This made sense as we're most comfortable working with people with a similar style to our own. Unfortunately the performance of this type of team could never match that of a balanced team. Some clients specifically keep style information in mind when they recruit new team members. Each style brings important strengths.

The 'Technology'

As a consultant and coach I have used this 'technology' for over 25 years to help people:

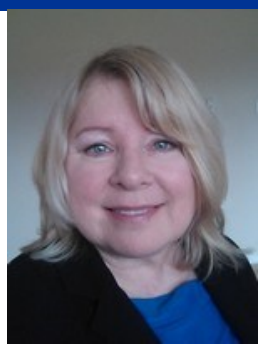
- learn about how others see them
- understand why they 'don't get along' with some people
- become aware of how others respond to them
- notice how their behavior changes under stress
- learn how to make others more willing to listen
- improve how a team works together
- design more persuasive presentations

This article is reproduced from the February 2015 edition of ***TMC's Advisor***

Thomi Glover, MA, MDiv, PCC, CMC *is a Certified Executive coach with over 3000 hours of individual and team coaching experience. She is a Leadership and Management Consultant and a specialist in Emotional Intelligence. Client comments include: "...the most effective executive coach I've worked with in my 35 year career" and "Without her coaching I would not have achieved the success I did."*

Data @ Large: The Real World of Data, Privacy and Security

By Ellen Koskinen-Dodgson



The 16th Annual Privacy & Security Conference was held this month at the Victoria Conference Centre. It was a great success with the primary message being that the world is scary, from a privacy and e-security point of view and it's getting scarier. From the introduction of Arpanet a scant 45 years ago to the internet that we know – things are much worse than I thought.

We Aren't Ready for the Future

Speakers told us about:

- how it isn't just hard drives that contain user data - using the example of the Guardian newspaper that found that they needed to destroy hard drives, keyboard controllers and other components as it all contained user data
- 'security updates' from false sources that reduced security, and how Internet of Things devices received these updates without any requirement for a human 'click to accept' response
- how there is expected to be at least 20 Billion hijack-able Internet of Things devices in use by 2020 including:
  - ◊ baby monitors and web cams
  - ◊ thermostats
  - ◊ ovens and fridges
  - ◊ door locks
  - ◊ sprinklers
  - ◊ even light bulbs and electrical outlets
- televisions that spy on us to collect saleable marketing information
- carriers that track turned-off mobile phones
- fake transmitters in a truck that find out who owns every mobile phone in a target range
- the popular joke of the self-driving car that drove a drunk guy home from a party but he woke up in a 7-11 parking lot because the fridge and told the car to stop for milk on the way home
- 'free' WiFi hotspots that front man-in-the-middle data hijacking
- how Google and its competitors know how to monetize all the data that flows through their systems
- how 55% of US people (less in Canada) would share personal information if receiving a 'benefit'
- how the default for privacy in the UK is that people will share their information
- how self-driving cars are simply waiting for laws to change
- the creepiness of how massive amounts of user data is analyzed to predict future behaviour
- how we need to assume that breaches *will* occur and to test security breach plans in the same way that we test emergency plans
- how police, policy-makers and law-makers need to learn to operate in this emerging new world
- how governments are struggling to find ways to protect our privacy and keep the Googles of the world from manipulating the marketplace and our buying decisions far into the realm of creepy

And My Presentation?

As my presentation was midway on the final day of the conference, I found that a number of speakers had stolen my thunder.

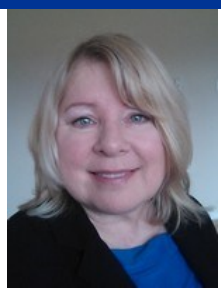
I didn't want to bore the attendees, so I shifted my talking points from a strictly technical presentation to a presentation on the human behaviour-security tug-of-war, a topic that is dear to my heart.

This article is reproduced from the February 2015 edition of ***TMC's Advisor***

Ellen Koskinen-Dodgson is President and Managing Partner of TMC IT and Telecom Consulting Inc. She is an IT and Telecommunications Management Consultant, electrical engineer, author, speaker, media resource and Expert Witness.

The People Side of BYOD

By Ellen Koskinen-Dodgson



Most employees don't like corporate BYOD policies. They love the idea of BYOD but they resent the restrictions that come with it. Resentful employees cause major security risks but so do the everyday employees who are too trusting, who think that the sky will never fall. Here are some ways to improve employee behaviour.

BYOD Basics

When an organization adopts BYOD, they first develop a mobility strategy. The outcome of the strategy is a set of policies along with technologies and procedures to implement the policies.

What Do Policies Say?

Policies identify which devices are available for BYOD, which apps are required, allowed and not allowed. It explains any compensation provided by the company for shared use, who owns the data and the rights of the organization to control of the device. It also explains acceptable use, which is the critical part of the document as it requires employee compliance. The acceptable use terms are all of the employee behaviours that protect the security of company data and access into their network. At a minimum, the policy should require employees to:

- Register their personal devices before using them for company business.
- Use caution to avoid theft and notify the company promptly if their devices are lost or stolen.
- Protect their devices with a secure password.
- Do not 'jailbreak' their devices to or otherwise remove protections.
- Do not download unauthorized apps.
- Install (and keep updated) security software, such as antimalware and remote-wipe applications.
- Only access the company network using an approved method, such as a VPN.
- It may require reporting any 'suspicious' actions by their device as this may be a security problem.

User Need to be Sold

Employees will sign a BYOD policy document in the same way that they click 'accept' on their Facebook agreement. Most don't actually read it. Most of those that do, don't understand it all. Of those that understand some of it, few remember the contents for very long.

For a BYOD policy to be effective, the document needs to be more than the agreement for a new app. It needs to be reviewed in person with each point explained properly, including why the point is included in the policy. Penalties for violating the policy should also be reviewed. Further to this, employees need to be regularly reminded through case studies or other teaching tools in a classroom setting or in departmental meetings.

Painful Lessons

There's nothing worse than an employee realizing what a policy means through a painful lesson. Lessons might include:

- Your company has come under investigation and employee mobile phones and devices have been seized for investigation. That means that strangers could 'paw through' their photos and other personal data.
- They misplace their tablet and report it missing, then realize that all of the contents of the tablet have been remotely wiped, which include the only copies of:
    - important family photos
    - all of their personal contacts
    - personal appointments
    - personal emails
    - their password list
    - their wife's partially completed novel
- They arrive at work and find out that they've been terminated for violating the BYOD policy that they signed as 'proof' that they had read all of it.
- The police arrive at their door to arrest their son for maliciously hacking into the company's computer using their 'shared' tablet.

This article is reproduced from the February 2015 edition of ***TMC's Advisor***

Ellen Koskinen-Dodgson is President and Managing Partner of TMC IT and Telecom Consulting Inc. She is an IT and Telecommunications Management Consultant, electrical engineer, author, speaker, media resource and Expert Witness.