Maner Costerisan
Certified Public Accountants
Business & Technology Advisors

I.T. THAT GOES BUMP IN THE NIGHT!

Ryan Carter, CNA, CNLM,
Senior Information Technology Consultant
(517) 886-9526
rcarter@manersolutions.com

Notable quotes about technology's role in the downfall of mankind....

- "We can't jump off bridges anymore because our iPhones will get ruined. We can't take skinny dips in the ocean because there's no service on the beach and adventures aren't real unless they're on Instagram. Technology has doomed the spontaneity of adventure and we're helping destroy it every time we Google, check-in, and hashtag."
  — Jeremy Glass

- "If privacy had a gravestone it might read: 'Don't Worry. This Was for Your Own Good."
  — John Twelve Hawks, The Dark River

- "The production of too many useful things results in too many useless people."
  — Karl Marx

- "Remember when only a few people had mobile phones. Generally regarded as an object of derision, you would occasionally see business types clutching those ridiculous grey bricks to their faces and mutter to yourself 'what a prick.' Nowadays, an eyebrow hardly even flutters when we see a ten-year-old child happily texting away. — Simon Pegg, Nerd Do Well

- "E-mail has some magical ability to turn off the politeness gene in a human being."
  — Jeff Bezos

Maner Costerisan
Certified Public Accountants
Business & Technology Advisors

Who am I?

Ryan Carter, CNA, CNLM
rcarter@manersolutions.com
517-886-9526
Http://bit.ly/2wSsW60

- Team member of the Maner Business and Technology Solutions Group.
- Senior Infrastructure Engineer w/Maner since 2016.
- Over 25 years experience in the IT field, started in 1990.
- Certificate in Non-Profit Leadership and Management thru MSU, ITIL v3 Certified, Scrum Certified, Certified Novell Admin.
- Held Executive Director level positions in Non-profit, Manufacturing, Insurance, State Government and IT Consulting sectors.
- Owned and operated an IT consulting practice since 1998.
- Focused practice with Cisco, VMware, Microsoft, FortiNet, Network Vulnerability Assessments.

Maner Costerisan

So what's so scary about IT...

- The pace at which new technology arrives on the market before it's been properly vetted and tested.
- Traditional manufacturing companies that jumped into technology.
- Technology advancements that make you scratch your head.
- Products touted by manufacturers that will ease the burden on everyday life. The better mouse trap.
- Explosion of wearable based products aimed at health tracking.
- The flood of home security and automation based products.
- Tools used to penetrate Wi-Fi, networks, and security systems are free.

  (And have been for many years)

Maner Costerisan

Agenda….

- Wi-Fi – Public use, open free, hotels, and hidden dangers
- Ransomware – How it works
- Ransomware – The face of the new attacker
- Vehicle security – Connectivity and software flaws
- IoT attacks – How easy they are
- Smart Guns – Not really…
- Resources – Helpful links and sites

Maner Costerisan

Maner Costerisan

Video produced by Kaspersky Labs.

Wi-Fi OMG!

- At each convention(DNC and RNC)private entities provided visitors with free public Wi-Fi networks and around 70 percent of people connected to the un-secure Wi-Fi networks at both conferences.
- In 2016, 87 percent of US consumers use public internet, and more than 60 percent believe their information is safe on public Wi-Fi. Just half believe they must secure their own information, with 17 percent thinking websites must protect their data, and another 17 percent thinking it is the responsibility of the Wi-Fi provider.
- The largest users are age 25-34 and 55-64.
- 75 percent of consumers don't use a Virtual Private Network (VPN) to secure their Wi-Fi connections, even though it's one of the best ways to protect your information.

Maner Costerisan

Wi-Fi tips . . .

- Don't use public Wi-Fi to shop online, log in to your financial institution, or access social media sites — *ever*
- Use a Virtual Private Network, or VPN, to create a network-within-a-network, keeping everything you do, type and view encrypted
- Implement two-factor authentication when logging into sensitive sites, so even if malicious individuals have the passwords to your bank, social media, or email, they won't be able to log in
- Only visit websites with HTTPS encryption when in public places, as opposed to lesser-protected HTTP addresses

Maner Costerisan

Wi-Fi tips continued...

- Turn off the automatic Wi-Fi connectivity feature on your phone, so it won't automatically seek out hotspots named the same as it's connected to in the past
- Monitor your Bluetooth connection when in public places to ensure others are not intercepting your transfer of data
- Buy an unlimited data plan for your device and stop using public Wi-Fi altogether, or use a cellular hotspot

Maner Costerisan

Ransomware – So what is it?

Maner Costerisan

Video created and produced by Enigmasoftware.com

Ransomware discussion

- Ransomware is designed to extort money from victim's by requiring payment in crypto-currency in exchange for a decryption key used to unlock the files encrypted by the attacker on the victims computer.
- At this stage of ransomware threats, criminals no longer target specific home or business sectors. Although the current trend is small local governments, municipalities and hospitals, originally the targets were home users.
- Targeted approaches that have surfaced today use a strong arm technique. Pay the ransom or the breach event will be leaked to the public causing embarrassment and loss of business. This is specifically dangerous to local governments, municipalities and hospitals as they typically house mass amounts of private citizen information, police records, medical information and credit info.
- The reasoning for targeting smaller sized organizations is that they typically don't have the technical staff onsite to combat the outbreak, limited IT budget spent on keeping the environment current / up-to-date, and a perceived willingness to pay to make the problem go away.

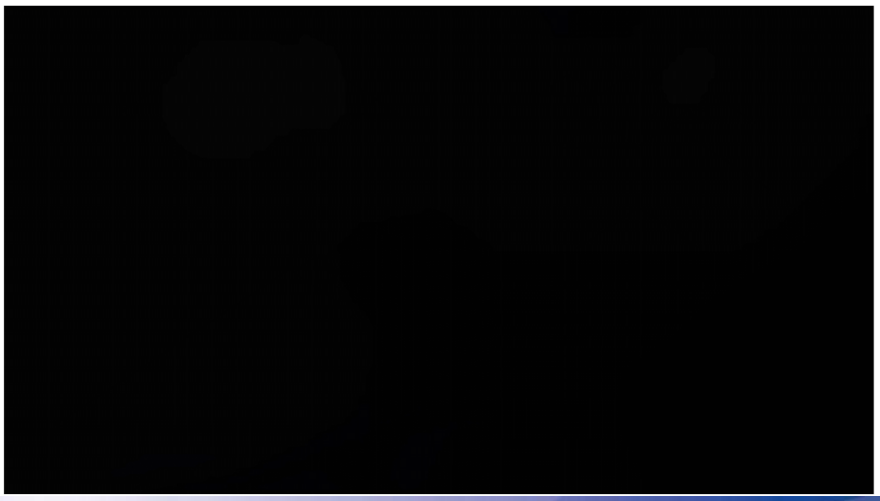
Maner Costerisan

Ransomware discussion continued...

- Vulnerability Assessment – Contract an IT firm to perform a non-biased vulnerability assessment survey of your IT environment. Follow any recommendations made by the assessment to close up gaps in your environment. *This is the first step to understanding where to start, focus recourses and make improvements*
- End user training – Knowledge is power when dealing with the topic of Ransomware and malware. Engaging in a robust training regiment to keep users up-to date on tactics used by cyber criminals is the best first line of defense. This includes mock spear phishing campaigns aimed at tracking which employee clicks on suspicious attachments, training videos on how Cryto-ware works and spreads, understanding attachments types, the ability to identify poorly worded or fake emails, and safe click habits when browsing social websites.
- Patches, Patches, Patches – Keep software patches up-to date on all systems, including systems that run lightweight Linux and Unix software. Microsoft software is the biggest target for cyber-criminals so make sure to have a solid patch strategy in place to keep Microsoft Windows updated using either Microsoft Update Services or an MSP managed care provider.
- Tested, reliable data backups – This step alone is the only way to recover from a crypto-ware attack! Make sure you have a solid data backup methodology documented, tested and verified. Review this strategy, make sure everyone understands what will happen in the event of a data breach, perform data restores once a quarter to verify the data backed up can be recovered. Make sure systems used to perform backups are locked down from user access, and utilize non-admin accounts to perform backups.
- Passwords – *Adopt and enforce a strong password policy* including a timely rotation plan, 90 or 120 days. One such policy includes choosing eight random words, using the first letter of each word, substituting 2 letters with special characters, add in 2 numbers, and capitalize 2 of the letters. Passwords should never be written down, or shared with anyone. Do not use one password across all technology locations, select a different password for online use, separate from email, or network login's. Avoid using pet's names, kids names, or the word password!

Maner Costerisan

So what does an attacker look like?



This video was produced and created by Cisco Systems

Attacker discussion

- Today's attacker could realistically be anyone. Motivations range from just for kicks, money, a sense of power, showing off their technical prowess, to a grudge against a competing company or business.
- Studies show the *predominate* traits of a hacker today are: Male, early 30's, white and generally low to middle class.
- Location no longer matters, attackers are global and range across all countries. Due in part to the explosion of low cost internet connectivity, inexpensive computers along with free widely distributed hacking tools.
- Criminal families and the proliferation of RaaS attract anyone with any technical ability to use their skillset to earn a slice of the take.

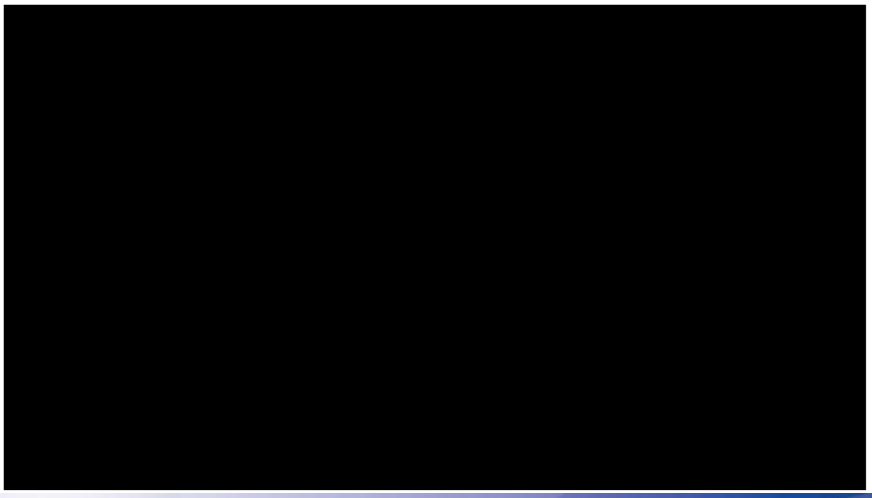
Vehicle security

This video was created by Wired.com

Vehicle safety discussion

- By 2020, virtually all manufactured vehicles will come with embedded, tethered or smartphone mirroring connectivity. Already in the first quarter of 2016, cars accounted for one-third of all new cellular devices.
- Fiat Chrysler Automobiles (FCA), the world's seventh largest automaker, issued a recall notice for 1.4 million vehicles in order fix a software hole that allowed hackers to wirelessly break into the Jeep Cherokee and electronically control vital functions.
- What does loom as a larger threat for example, a hacker could encrypt a vehicle's infotainment system, denying access and then blackmail either the vehicle owner or the carmaker to release it.
- For terrorists, the potential to shut down a fleet of vehicles or a transportation system would be considered low-hanging fruit.
- Hackers have taken remote control of a Tesla Model S from a distance of 12 miles, interfering with the car's brakes, door locks, dashboard computer screen and other electronically controlled features in the high-tech car. (2016)

IoT, how I love thee'



Maner Costerisan

This video was produced and created by Cisco Systems

IoT discussion

- A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.
- IoT devices we might use now in our daily lives: Amazon Echo, Google Home Mini, Amazon Fire Stick, Tide "Dash" Button, Schlage door locks, Tile, Belkin WeMo smart electrical outlets and wall switches, Wi-Fi lighting, Nest thermostats, MyQ wireless garage door openers, GE appliances (refrigerators, ovens), Ring doorbells and webcams, Fitbit, Samsung VR, Apple Watch…
- Researchers at Microsoft and the University of Michigan recently found a plethora of holes in the security of Samsung's SmartThings smart home platform, and their methods were far from complex.
- FTC report found that companies could use collected data that consumers willingly offer to make employment decisions. For example, an insurance company might gather information from you about your driving habits through a connected car when calculating your insurance rate. The same could occur for health or life insurance thanks to fitness trackers.

Maner Costerisan

The best intentions...

Maner Costerisan

This video was created by Wired.com

IdiOTic.... Seriously?

"A DXV smart toilet will bring your bathroom to the cutting edge of cleanliness".

For decades you've been able to adjust just how dark you want your bread with a knob or lever. But maybe we've been missing out on perfect toast because we didn't have the opportunity to *really* fine-tune the cooking experience.

The Coach, according to those behind it, has been designed to "reinvent what a person's relationship with their hair can look like".

The HapiFork is a Bluetooth-enabled "smart fork" that vibrates when it senses you're eating too fast.

Maner Costerisan

Resources

- To file a cyber crime complaint with the FBI: https://www.ic3.gov
- To test the strength of your password: http://www.passwordmeter.com/
- Password best practices: https://krebsonsecurity.com/password-dos-and-donts/
- Vulnerability Assessment Information: http://manersolutions.com/services/vulnerabilityassessment
- End user security awareness training: https://www.knowbe4.com/
- Security bulletins and vulnerability announcements: https://www.us-cert.gov/ncas/bulletins
- DOJ best practice PDF on Ransomware: https://www.justice.gov/criminal-ccips/file/872771/download
- Has your email account ever been hacked: https://hacked-emails.com/

Maner Costerisan
Certified Public Accountants
Business & Technology Advisors

Ryan Carter, CNA, CNLM,
Senior Information Technology Consultant
(517) 886-9526
rcarter@manersolutions.com

QUESTIONS?

rcarter@manersolutions.com
517-886-9526

Maner Costerisan
Certified Public Accountants
Business & Technology Advisors