



K2's Ethics And Technology



Tommy Stephens



CPA from Woodstock, Georgia

Partner, K2 Enterprises

Thirty-eight years public accounting & private industry experience

BSBA (Accounting) Auburn University

MS (Finance) Georgia State University

Please contact me: tommy@k2e.com

Follow me on Twitter: [@TommyStephens](https://twitter.com/TommyStephens)

Learning Objectives



Distinguish between
ethics and morals

Define “technoethics”
and identify examples of
business ethics issues
and how they are
affected by technology

Recognize the influence
of technology on ethics
requirements in Codes
of Conduct

List at least five
examples of potential
ethics issues associated
with leading
technologies today

Major Topics Covered



Differentiating between morals, ethics and laws

Examining key provisions of accountants' Code of Conduct

Reviewing notable technoethics issues and cases

Creating a culture that advances ethics

Laws, Morals, & Ethics



Laws

- *Created by others*
- *Influenced by us as citizens and voters*

Ethics

- *Created by others and by our chosen profession*
- *Influenced by us and our chosen profession*

Morals

- *Created by us*
- *Influenced by family, friends, teachers, others and, for many, faith*

Looked At It A Little Differently...



*“Ethics is knowing the difference
between what you have a right to do,
and what is right to do.”*

*“Ethics is doing the right thing when no
one else is looking.”*

Eight Components Of A Mature Professional Infrastructure



- | | |
|-----------------------------------|-----------------------------|
| 1. Initial professional education | 5. Licensing |
| 2. Accreditation | 6. Professional development |
| 3. Skills development | 7. Code of ethics |
| 4. Certification | 8. Professional society |

As identified by Gary Ford and Norman Gibbs in “A Mature Profession of Software Engineering,” 1996, Carnegie Mellon University



CODE OF PROFESSIONAL CONDUCT

Six Principles Of The AICPA Code Of Professional Conduct



Responsibilities
Principle

Public Interest
Principle

Integrity Principle

Objectivity and
Independence
Principle

Due Care
Principle

Scope And
Nature of
Services Principle

Code Of Professional Conduct



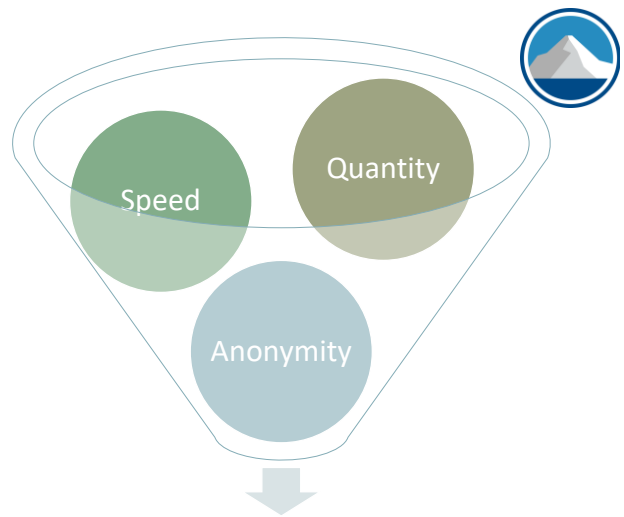
- AICPA's Code of Professional Conduct is applicable to **all** members of the organization, in performance their *professional responsibilities*, irrespective of whether they are in public practice, industry, governmental, or other organizations
 - Note the emphasis above on professional responsibilities...it does not apply to personal matters
- However, a large portion of the Code focuses on members in public practice, particularly when performing attest engagements
- The word **“technology”** is mentioned only 4 times in the 218 page document that codifies the standards and even then, it is not used in the context of “technoethics”

Code Of Professional Conduct



- AICPA's Code of Professional Conduct is applicable to **all** members of the organization, in performance their *professional responsibilities*, irrespective of whether they are in public practice, industry, governmental, or other organizations
 - Note **Safe to say, we don't have a lot of authoritative guidance in this area** not apply to pe
- However, a large portion of the code focuses on members in public practice, particularly when performing attest engagements
- The word **“technology”** is mentioned only 4 times in the 218 page document that codifies the standards and even then it is not used in the context of “technoethics”

How Does Technology Impact Ethics?



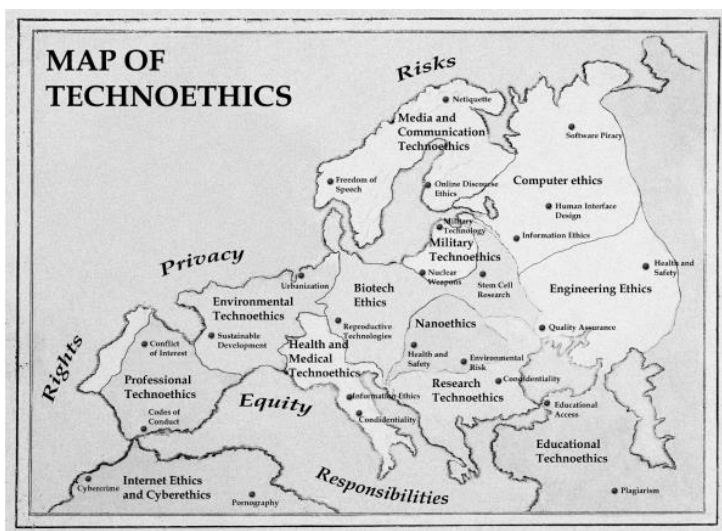
Greater Opportunity? Greater Temptation? Greater Reward From Potentially Unethical Actions?

Technoethics Definition



Using theories and methods from multiple domains, technoethics provides insights on ethical aspects of technological systems and practices, examines technology-related social policies and interventions, and provides guidelines for how to ethically use new advancements in technology.

https://en.wikipedia.org/wiki/Ethics_of_technology#Definitions



K2 Enterprises

Jacobus Lentz, IBM, And The Nazis: *An Early Case In Technology Ethics*

- Inspector of Population Registries in Netherlands prior to World War II
- With leased IBM machines, he created forgery-proof ID cards
- After German invasion, cards were issued to all
- Lentz also created an alphabetical listing of Jews in the Netherlands, which was used beginning in 1942 to facilitate deportation of Jews to concentration camps
- 107,000 were deported and of these persons, 102,000 died



Page 7

Copyright © 2023, K2 Enterprises, LLC.

Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

Napster: A Case In Technology Ethics



- Do you remember Napster, the online, peer-to-peer network that facilitated sharing music MP3s?
- Service operated between 1999 and 2001
- Metallica filed suit in March 2000 against Napster; Dr. Dre filed similar suit one month later
 - Napster settled both suits
- A&M Records through the RIAA sued Napster in 2000 for copyright infringement and Napster lost that case
- Napster shut down in 2001 and sold off assets in 2002

Consider What Sony Did In 2005



- *In an effort to be proactive rather than just litigious in limiting illegal online music swapping, the label late last year tried something new: music CDs that when placed in a customer's computer installed a program to prevent the copying of songs. Companies have been adding antipiracy features to products for years, so what's wrong with that? Everything, according to an outraged mass of music fans. Installing software programs--even (or perhaps especially) one aimed at protecting intellectual property--without explicit user permission turned out be crossing the line. Even worse, the software made computers vulnerable to viruses. Sony quickly backed down and offered a program to remove the first one. But it just ended up making things worse when the new program was found to have similar security flaws.*
<https://www.inc.com/magazine/20060301/column-freedman.html>

Clearview AI



Computer
vision for a
safer world

[Request Access](#)

- **Public information only.**

- Clearview AI searches the open web. Clearview AI does not and cannot search any private or protected info, including in your private social media accounts.

What Do The Cases Have In Common?



Cutting-edge
technology
(at the time)

Volume of
data

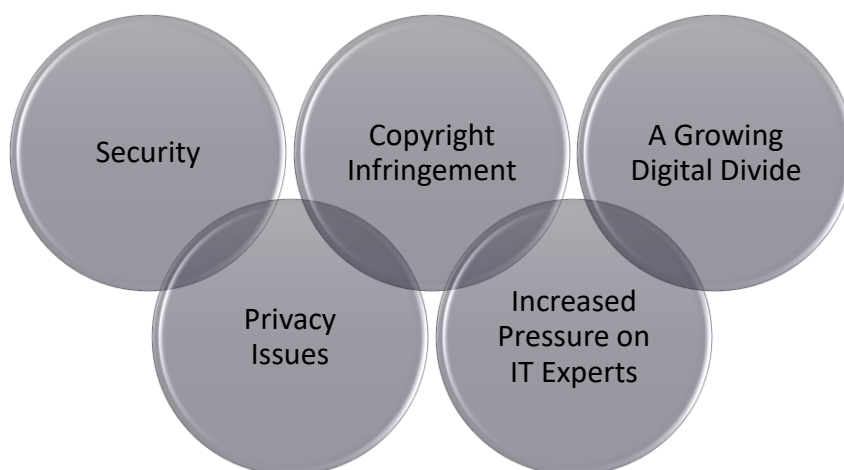
Speed of
processing

Privacy of data



JUST AS TECHNOETHICS EVOLVED FROM 1940 TO 2000, IT CONTINUES TO EVOLVE TODAY, BECAUSE OF CONTINUAL TECHNOLOGY ADVANCEMENTS AND INITIATIVES...

Technoethcis: Five Challenges



Karehka Ramey, <https://www.useoftechnology.com/5-ethical-challenges-information-technology/>



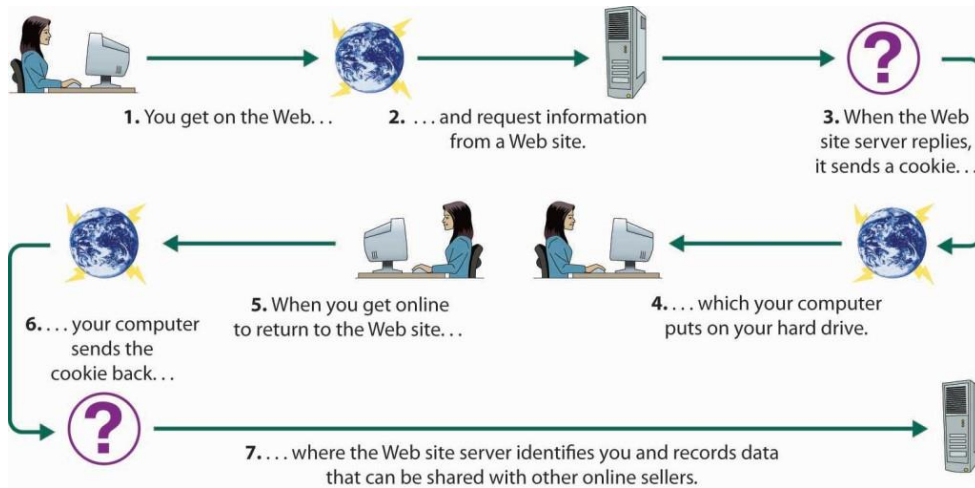
SOME EXAMPLES TO SEE WHAT TECHNOETHICS LOOKS LIKE...



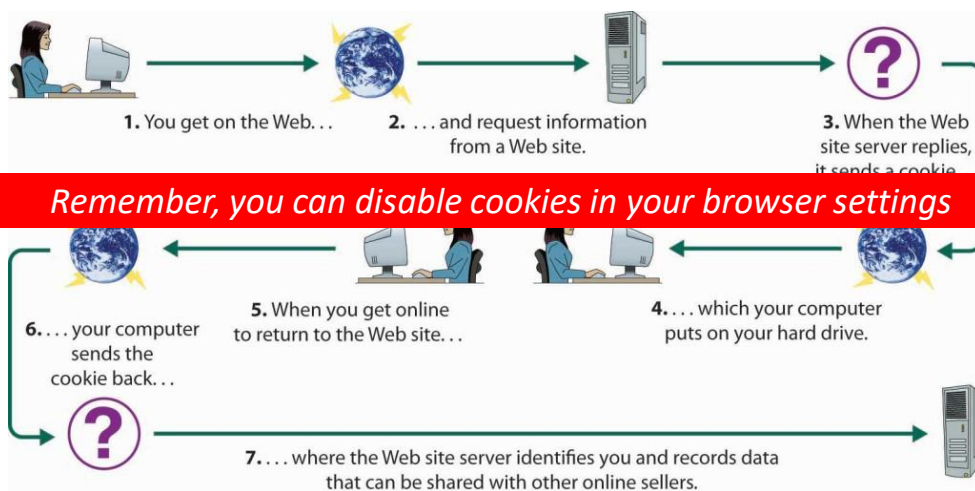
What About Privacy Of Consumer Data?

- How much does Google, Amazon, Microsoft, Facebook, and other companies know about you?
- How do they collect this info and what can you do about it?
- What about your choice of a search engine? Does it matter?
- Are these technology companies acting ethically when they collect data about you?

How Do Cookies Collect Your Info?



How Do Cookies Collect Your Info?

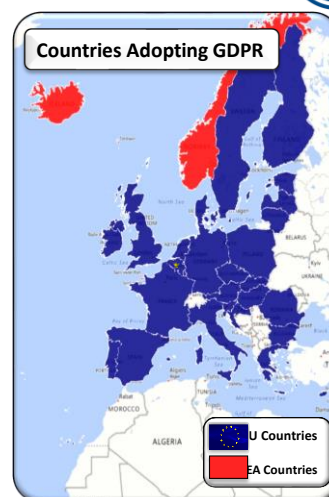




WHAT IS GDPR AND WHAT DOES IT MEAN TO ME?

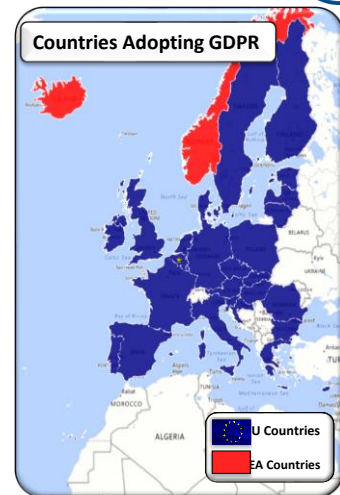
What Is GDPR?

- The General Data Protection Regulation (GDPR) of the European Union
- In effect as of May 25, 2018
- One of the first in an expected global wave of data governance laws which regulates how companies use your personal data
- Makes it unlawful to collect or transfer data on EU citizens unless the organization meets certain conditions and either submits to EU regulation or modifies its business processes
- Data collection and processing must be done by consent or for specific reasons permitted by law



What Is GDPR?

- Gives users rights to view, control, transfer, and demand erasure of their data, which will require organization and cataloging to determine what information your organization has and uses
- Imposes requirements and penalties for noncompliance on companies worldwide – depending on type/severity of violation, fines can be up to the higher of:
 - €10-20 million (depending on the type and severity of violation)
 - 2-4% of worldwide sales



GDPR's Major Requirements

- Processing of personal information must be done under one of six allowable reasons for data processing under the statute, and some types of data have more limitations
- When a subject consents to data processing, the consent must be
 - Clear about the information gathered, and
 - Explicitly state the purposes for which it is to be used
- Subjects can withdraw their consent to data processing at any time
- Subjects have the right to submitting corrections to data
- Organizations must name a Data Controller, a Data Protection Officer and potentially other employees to roles over data governance

GDPR's Major Requirements



- Data subjects have the right to receive a copy of all data retained by an organization on them upon request within 30 days
- Data subjects have the right to not be classified based on an automated processing
- Subjects have the right to erasure of their personal data upon request
- Any stored data must be portable and able to be transferred to another system upon request
- Data regulators must be notified within 72 hours of any data breach – even if the data is encrypted – but individuals may or may not have to be notified in that timeframe
- Documentation of the data stored and logs of the processing activities must be maintained if the company has over 250 employees

Who Is Covered By GDPR?



- All data stored in EU countries and all personal data for EU nationals, regardless of location are covered
- All organizations which have a data controller, data processor, or a data subject in the EU are covered
- All organizations which collect or process data on EU citizens, regardless of location



Data Privacy & Security By Default

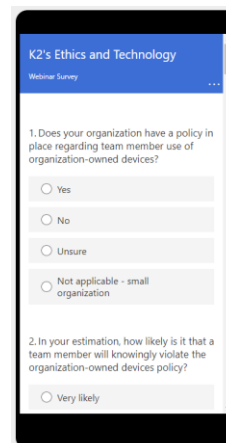


- GDPR recommends that those subject to GDPR limit the data they keep, and not keep certain sensitive data unless it is necessary
- Data controllers are required to implement processes which implement data privacy by design/default and data security by design/default
- These procedures require that processes like the anonymization of personal data are considered and implemented if appropriate into the organization's business processes and data stores

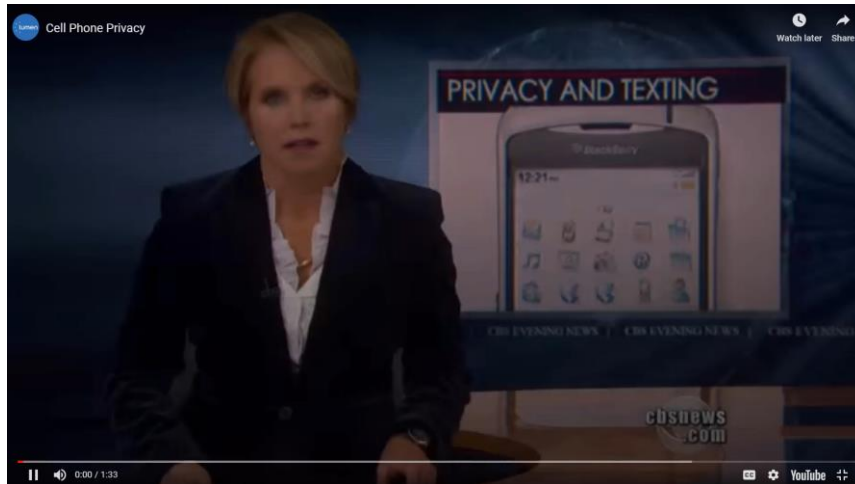
Use Of Company-Owned Devices



- Is it safe to say that almost all workers with access to company-provided technology use these tools for personal reasons?
- What if this is in violation of company-established policies?
- What if this causes inefficiencies and lost productivity and simultaneously increases risk?



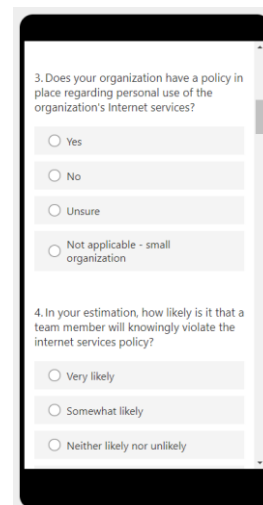
Technology And A Right To Privacy



Personal Use Of Company's Internet



- Virtually every business is connected to the Internet today
- Team members often take advantage of Company-owned Internet access for personal activities, perhaps in violation of Company-issued policies
- It's not just a *quantity* issue, it is also a *quality* issue – what types of sites are they visiting?



3. Does your organization have a policy in place regarding personal use of the organization's Internet services?

☐ Yes

☐ No

☐ Unsure

☐ Not applicable - small organization

4. In your estimation, how likely is it that a team member will knowingly violate the internet services policy?

☐ Very likely

☐ Somewhat likely

☐ Neither likely nor unlikely

Personal Texts And Social Media Posts



- Like it or not, social media is here to stay
 - In fact, many businesses have incorporated it as a major component of their communication and marketing strategies
- But how much time are team members spending each day texting and posting personal content?
- Is this acceptable?

5. How often do you send personal texts and/or social media posts while at work and during normal working hours?

☐ Daily

☐ Weekly

☐ Never

6. In your estimation, how likely is it that a team member will spend more than an hour each day engaging in personal texting and social media updates?

☐ Very likely

☐ Somewhat likely

☐ Neither likely nor unlikely

☐ Somewhat unlikely

☐ Very unlikely

Can Employers Require Social Media Access?



Password And Access Policies



- No one likes passwords, but they remain a “necessary evil” today
- In far too many organizations, team members routinely share passwords with others
 - For example, during vacations
- Also, many team members do not follow password policies in organizations, potentially increasing risk to their employer

7. In your workplace, how frequently are passwords shared among multiple team members?

☐ Frequently

☐ Occasionally

☐ Rarely, if ever

8. Do you personally adhere to your organization's password policy?

☐ Yes

☐ No

☐ Unsure

☐ Not applicable - small organization

Company's Use Of Monitoring Tools



- How often, if ever, does your organization use monitoring tools to keep an eye on what team members are doing with their technology?
 - For example, what websites are being visited?
- What would be the benefit to the organization for doing so?

9. Does your organization monitor your use of technology?

☐ Yes

☐ No

☐ Unsure

☐ Not applicable - small organization

10. Have you or someone you work with ever been disciplined for improper use of technology in the workplace?

☐ Yes

☐ No

☐ Unsure

Copying And Pasting Information



- It's all too easy to copy-and-paste information from the Internet without proper attribution, perhaps in violation of copyright laws
 - Remember Napster?
- Similarly, scanning and running OCR on PDF documents could lead to the theft of someone's intellectual property

11. In the past year, have you knowingly copied and used copyrighted information from the Internet without appropriate attribution?

☐ Yes

☐ No

☐ Unsure

12. As an individual, how do you feel when a company you do business with is using your data to sell you more products/services?

☐ Very positive

☐ Somewhat positive

☐ Neutral

☐ Somewhat negative

Collecting Information About Customers And Potential Customers



- Privacy is a huge issue today
- What do companies such as Google, Microsoft, Amazon, and others know about you?
- What type of information is your company collecting about customers and what is being done with that data?
- Is this disclosed in your company's Privacy Policy?

12. As an individual, how would you feel if a company you did business with was harvesting personal data about you and using it to attempt to sell more products/services to you?

☐ I would be very upset, to the point I would cease doing business with that company

☐ I would be moderately upset, but would continue to do business with that company

☐ I would not care

13. How often do you work from home or other non-corporate locations?

☐ Daily

☐ Weekly

☐ Monthly

Issues Surrounding Remote Workers



- Large numbers of team members work from remote locations, for many reasons
- This leads to numerous potential ethical issues
 - Are they really working when they're supposed to be?
 - How are they using their technology?
 - Are they being treated fairly, and are their contributions valued?

13. How often do you work from home or other non-corporate locations?

☐ Daily

☐ Weekly

☐ Monthly

☐ Seasonal

☐ Never

14. When away from the office, how do you access organization information? (select all that apply)

☐ Smartphone

☐ Tablet

☐ Laptop

Internet Access In Remote Areas



- When working outside away from the office, how do you access the Internet?
 - Cellular data
 - Public Wi-Fi
 - VPN
- Do you comply with company-issued standards/best practices and, if not, what's the risk?

14. When away from the office, how do you access organization information? (select all that apply)

☐ Smartphone

☐ Tablet

☐ Laptop

☐ Desktop

☐ Not applicable

15. Is that access done in accordance with organization-issued standards, including firewalls, non-public connections, etc.?

☐ Yes

☐ No

☐ Not applicable

Sensors And Cameras



- What type of sensors and cameras exist in your workplace, if any, in the name of security?
- Could these be used for unethical purposes?
- What about the potential benefits associated with using facial recognition in law enforcement situations?

16. How do you feel about sensors and cameras monitoring your actions in the workplace?

☐ Very positive

☐ Somewhat positive

☐ Neutral

☐ Somewhat negative

☐ Very negative

17. Away from work, how do you feel about sensors and cameras monitoring your actions in public places, such as when walking on a sidewalk?

☐ Very positive

☐ Somewhat positive

☐ Neutral

Illegal/Unlicensed Computer Software



- Just because someone bought a license to an application doesn't give them the right to install it onto an unlimited number of devices
- Likewise, subscription services may have restrictions on sharing of the service

18. Have you ever installed software onto a computer - at work or at home - for which you or your organization did not own a license to use the software?

☐ Yes

☐ No

☐ Unsure

19. Have you ever used any type of Cloud-based tools in violation of the End User License Agreement?

☐ Yes

☐ No

☐ Unsure

20. Thank you for participating, please provide any additional comments you



ETHICAL LAPSES IN THE DIGITAL AGE OFTEN RESULT IN FRAUD AND SECURITY BREACHES

An Example...



Medical bills and lost time away from work caring for a critically ill child have created a financial hardship for Tim and his family; they face enormous financial hardships. With his back to the wall, Tim sees no way out and he decides to steal from his employer. Because the Controller keeps their passwords on a sticky note on the side of their monitor, Tim is able to use those credentials to log-in to the Company's accounting system and begin committing a billing scheme fraud. Eighteen months later, the fraud is discovered after Tim has stolen more than \$100,000 from the Company. Sure, Tim had an ethical lapse and committed a crime, ***but what can we say about the Controller's ethics in this case?***



CAN WE AGREE THAT ALL CASES OF FRAUD REPRESENT ETHICAL LAPSES?

Findings From The ACFE



- Occupational fraud consumes 5% of all business revenues
- Annual occupational fraud losses approximate \$4.5 trillion worldwide and \$1.08 billion in the United States
- On a per-employee basis, fraud costs on average \$8,244 per full-time worker, per year in the US and \$5,859 per full-time worker, per year in Canada
- The median loss for an occupational fraud in the US and Canada is \$120,000 (USD)



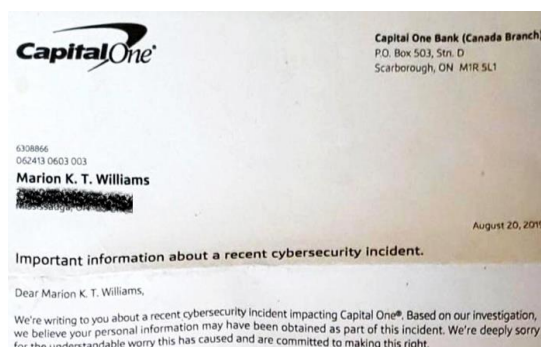
TECHNOETHICS & CYBERSECURITY

Cybersecurity – A Case Study



Capital One

- Capital One was hit with a data breach, affecting an estimated 100 million US individuals and 6 million in Canada
- Misconfiguration of a firewall allowed hacker access to the system



Ethical Issues



Integrity and Due Care

- Was the firewall rules reviewed by anyone and was any testing completed?

Professional Competence

- Did Capital One employ people with the correct skill set?
- Was consultation or referral required?

Objectivity

- Are you bias toward cloud and believed this was a cloud issue? This could be any office with a misconfigured firewall.



EMAIL

Email

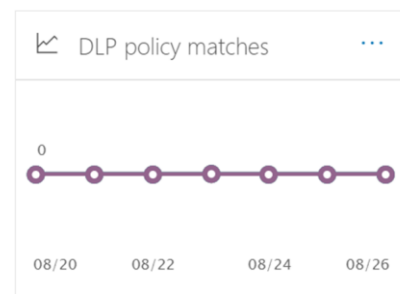


- Email remains one of the most used means of communicating amongst business professionals
- It's quick, easy, and widely accepted, so what are the ethical issues associated with this communication platform?
- Likely, the most significant of these issues is the security and privacy of the data transmitted in a message
- Absent encryption, we should assume that email messages are not secured, creating a risk for potentially exposing data

Data Loss Prevention



- Data Loss Prevention (DLP) can help identify, monitor, and automatically protect sensitive information
- DLP is available in many Microsoft 365/Office 365 plans, yet many organizations have not enabled it





DATA

Confidential Client Information



Per the AICPA Code of Conduct:

“... regulations concerning confidentiality of client information may be more restrictive than the requirements in the code.”⁽¹⁾

Consult your federal, state, provincial, and local privacy regulations.

Data Protection – An Example



- Dropbox files at rest are encrypted using 256-bit Advanced Encryption Standard (AES)
- Dropbox uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) to protect data in transit between Dropbox apps and our servers
- SSL/TSL creates a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption
- Dropbox applications and infrastructure are regularly tested for security vulnerabilities and hardened to enhance security and protect against attacks
- [Two-step verification](#) is available for an extra layer of security at login
- If you use two-step verification, you can choose to receive security codes by text message or from any Time-Based One-Time Password ([TOTP](#)) app, such as [those listed here](#)
- Public files are only viewable by people who have a link to the file(s)

Does Your Password Matter?

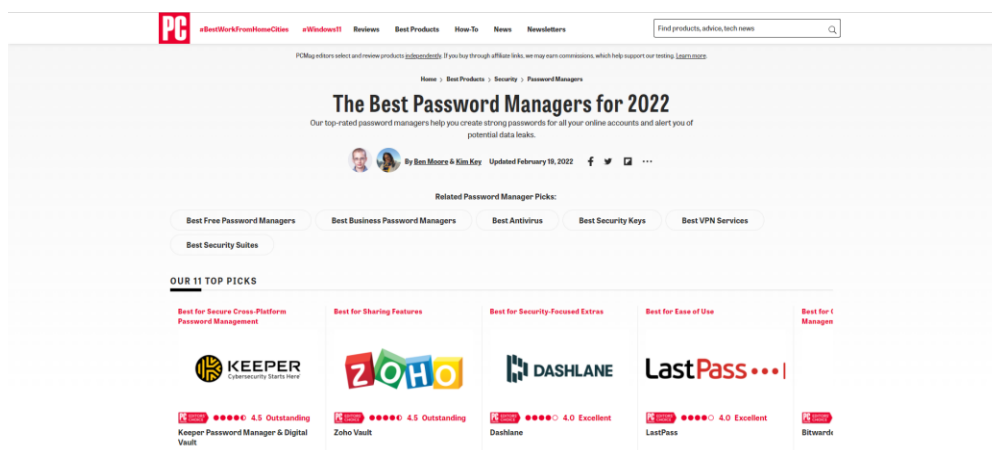


According to Microsoft:

“ – your password, in the case of breach, just doesn’t matter – unless it’s longer than 12 characters and has never been used before – which means it was generated by a password manager”

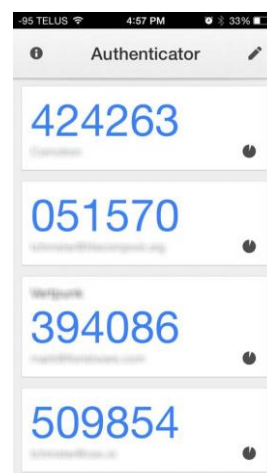
- What do you use to prevent access to your data – a password
- Do you use a password manager to provide due care and confidentiality of your data?

Strong Password Managers



Also, Per Microsoft

“your account is more than 99.9% less likely to be compromised if you use MFA”



Software Updates And Due Professional Care



- Equifax Breach
 - Hackers were able to access personal data of 143 million Equifax customers
- What Happened
 - **System update not installed**
 - “Equifax admitted it was aware of the security flaw a full two months before the company says hackers first gained access to its data” ⁽¹⁾



SO, WHAT ARE WE TO CONCLUDE ABOUT ETHICS IN AN AGE OF TECHNOLOGY?

Summary



- The issue of ethics in business is as old as business itself
 - Technoethics just takes it to another level
- With widespread deployments of technology, the ability to act can, in some cases, be more readily accessible and more easily concealable, leading to larger losses
- Who's to blame? **The perpetrator, always the perpetrator!**
- But we must accept the responsibility to act ethically and to promote ethics to reduce the risk to our companies
- Remember, we get to make choices too!



THANK YOU!