SOCIAL MEDIA SECURITY

A PRIMER – THAT CAN SAVES REPUTATIONS
01 Introduction
Why Social Media Security is important?

02 Threats and Plausible Issues
Threat Matrix and other issues with use of Social Media

03 Defensive Techniques
How to defend your organization

04 Legal Concerns and Preventive Issues
Legal concerns and a checklist of sorts
Making Cyber Hygiene a Priority

Unokha.co.nz
The precondition to FREEDOM is SECURITY.
CISOs of tomorrow will decide the bottom line of companies.
DIGITAL AROUND THE WORLD IN 2018

KEY STATISTICAL INDICATORS FOR THE WORLD’S INTERNET, MOBILE, AND SOCIAL MEDIA USERS

TOTAL POPULATION: 7.593 BILLION
INTERNET USERS: 4.021 BILLION
ACTIVE SOCIAL MEDIA USERS: 3.196 BILLION
UNIQUE MOBILE USERS: 5.135 BILLION
ACTIVE MOBILE SOCIAL USERS: 2.958 BILLION

URBANISATION: 55%
PENETRATION: 53%
PENETRATION: 42%
PENETRATION: 68%
PENETRATION: 39%

SOURCES: POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU; INTERNET: INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIAL.Org; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA; SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK; TENCENT; VKONTAKTE; KAKAO; NAVER; DING; TECHRASA; SIMILARWEB; KEPIDS ANALYTICS; WE ARE SOCIAL; Hootsuite; Hootsuite Analytics. NOTE: PENETRATION FIGURES ARE FOR TOTAL POPULATION (ALL AGES).

Source – Hootsuite.com
GLOBAL DIGITAL SNAPSHOT
THE LATEST NUMBERS FOR INTERNET, SOCIAL MEDIA, AND MOBILE USAGE AROUND THE WORLD

TOTAL POPULATION
7.524 BILLION
URBANISATION: 54%

INTERNET USERS
3.819 BILLION
PENETRATION: 51%

ACTIVE SOCIAL MEDIA USERS
3.028 BILLION
PENETRATION: 40%

UNIQUE MOBILE USERS
5.052 BILLION
PENETRATION: 67%

ACTIVE MOBILE SOCIAL USERS
2.780 BILLION
PENETRATION: 37%

SOURCES: POPULATION: UNITED NATIONS, U.S. CENSUS BUREAU; INTERNET: INTERNET WORLD STATS, ITU; INTERNET USER: INTERNET WORLD STATS, CIA; WORLD FACTBOOK; FACEBOOK; NATIONAL REGULATORY AUTHORITIES; TWITTER; WEibo; MIRRORONLINE; MOBILE: WE ARE SOCIAL; VIETNAM MINISTRY OF STATISTICS AND INFORMATION; EXTRAPOLATION OF EMARKETER AND ERICSSON DATA.

Source – Hootsuite.com
Social Media is indispensable
Social Media Risks
People share, read and engage more with any type of content when it’s surfaced through friends and people they know and trust.

Malorie Lucich
Legal and Regulatory Compliance

Disclosure of confidential information

Violation of Copyright laws

Non-compliance with industry regulations

Intellectual property rights
Brand and Reputation Damage

Unfavourable Content

Defamation

Copyright Infringement
Privacy Means

✓ Right to be left alone
✓ Limiting access to one’s personal information
✓ Secrecy
✓ Control over information
Social Media Defence
Safety, Security and Adherence
Simple Rules of Engagement

Prevention is Better than Cure
Guard Yourself
Check Before Posting

Your Post is PUBLIC
Corporate Espionage

Use of social engineering to access sensitive enterprise data
Assumed Trust

Willing to share personal information
Data Leak Using Apps

Collection of Personally Identifiable Information and use of AI
Other Common Issues

- Lack of consent
- Vulnerable participants
- Willful defaults
A Checklist of Don’ts

DON’Ts

• Complain publically about a specific person
• Post a picture without permission
• Tag someone in an embarrassing photo
• Write a negative post about a non-public figure
• Make any sexual references or Racial Slurs
• Doctor a photo
• Change the meaning of a post and repost it
• Post a private comment made in person
• Represent an original photo as your own
• Troll

A Checklist of Don’ts

DON’T

• Swear
• Hire or fire an employee through social media
• Reward one employee and not another
• Apologize to a specific person
• Post salary amounts for your staff
• Post vacation or business trip details
• Argue in public
• Link to inappropriate or crude content

A Checklist of Dos

DO

- Train your staff and yourself
- Get an audit done of your company’s social accounts
- Get professional help – when needed
- Get a social media security policy in place and tell people about it
- Check what apps are connected to your social accounts
- Monitor your social media regularly
- Limit access to only certain people – who matter

A Checklist of Dos

DO

• Practice your security worst case response strategy
• Check for fake stories
• Create Google Alerts to be aware of what is being published about your business
• Regular searches about yourself
• Protect End points – Mobile, Laptops, People
• Contact NZ Cert when an incident occurs

Concerns in NZ Context
A list of Issues that are commonly seen in the NZ Cyber Environment

- Corporate Espionage – Through People and Social Media
- Loose Lips and Data Leaks
- 3rd Party Apps leaking
- Privacy settings of employees
- Digital dossier aggregation
- Secondary data collection
- Difficulty of complete account deletion
- Phishing attacks
- Human error
New Zealand’s Privacy Act 1993

“when information is directly collected from an individual, the agency must make sure that the individual is aware of:

a) the fact that the information is being collected; and
b) the purpose for which the information is being collected; and
c) the intended recipients of the information; and
d) the name and address of the agency that is collecting the information; and
e) the agency that will hold the information; and
f) if the collection of the information is authorized or required by or under the law; the particular law by or under which the collection of the information is so authorized or required; and
g) whether or not the supply of the information by that individual is voluntary or mandatory; and
h) the consequences (if any) for that individual if all or any part of the requested information is not provided; and
i) the rights of access to, and correction of, personal information provided by these principles.
Under what circumstances can businesses access social media data?

“when information is directly collected from an individual, the agency must make sure that the individual is aware of:

a) the information is publically available, or
b) consent is obtained from the individual concerned, or
c) the information will be used for statistical or research purposes, or
d) the information will not be published in a form that could reasonably be expected to identify the individual concerned, or
e) compliance is not reasonably practicable in the circumstances of the particular case”
New Zealand’s Harmful Digital Communication Act 2015 (HDCA)

"a person may be held liable for spreading information that was already in the public domain (e.g., re-tweeting a defamatory tweet or sharing someone’s data which was deliberately made available by a hacker), given that it harms the individual whom the information is about, and it is unfair and unreasonable for a person to share that data.

The HDCA (which became law on 3 July 2015) is intended to discourage, prevent, and reduce harmful digital communications posted online through emails, text, websites, applications, or social media.
New Zealand’s Harmful Digital Communication Act 2015 (HDCA)

Here are the 10 principles of the HDCA:

**Principle 1**—a digital communication should not disclose sensitive personal facts about an individual.

**Principle 2**—a digital communication should not be threatening, intimidating, or menacing.

**Principle 3**—a digital communication should not be grossly offensive to a reasonable person in the position of the affected individual.

**Principle 4**—a digital communication should not be indecent or obscene.

**Principle 5**—a digital communication should not be used to harass an individual.

**Principle 6**—a digital communication should not make a false allegation.

**Principle 7**—a digital communication should not contain a matter that is published in breach of confidence.

**Principle 8**—a digital communication should not incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.

**Principle 9**—a digital communication should not incite or encourage an individual to commit suicide.

**Principle 10**—a digital communication should not denigrate an individual by reason of his or her color, race, ethnic or national origins, religion, gender, sexual orientation, or disability.
Law to your Aid

NZ Laws you need to be Aware of

New Zealand’s Unsolicited Electronic Message Act 2007
Regulates spam or junk or unwanted messages. To comply with the law
• Obtain Consent
• Provide Opt in and Opt Out options
Carry Home Points

- Conduct Social Audits
- Get a social media security policy in place and make it accessible
- Train your teams
- Abide by the Law
- Respect privacy
Questions??