Cybersecurity & Social Media Risk

Presented By:

Nejolla Korris

InterVeritas International Ltd.

Nejolla Korris, biography

Nejolla Korris is CEO of InterVeritas Intl. which provides lie detection, anti-corruption consulting, interviewing and interrogation training, investigative services, intelligence gathering, litigation support, linguistic statement analysis and employee audits.   .

Ms Korris is an international expert in the field of Linguistic Lie Detection. She is skilled in Scientific Content Analysis (SCAN), a technique that can determine whether a subject is truthful or deceptive. Korris has analyzed documents for fraud, international security, arson, sexual assault, homicide and missing persons' cases, causing some of her clients to dub her the "Human Lie Detector."

In 2011 she launched a series of seminars on social media risk and social engineering. In addition to providing training she consults with many corporations on social media audits and development of social media policies.

Korris provides training throughout North America, Europe, the Middle East, Malaysia, Brazil, Singapore, Botswana, Uganda, Kenya, Tanzania and South Africa. Her clients include corporations, government agencies, law enforcement and the military.

Ms. Korris is a popular speaker on Lie Detection, Fraud Prevention & Investigation, Workplace Fraud, Social Engineering and Organizational Justice. She is a frequent presenter for The Institute of Internal Auditors, ISACA, the American Society for Industrial Security, the American National Safety Council, the American Institute of Certified Public Accountants as well as several fraud prevention groups.

Nejolla has a BA in Law from Carleton University. Ms. Korris writes a column in Edmontonians magazine entitled *Civil War*s and has a blog entitled The Korrispondent.

www.interveritas.com

Part I

Social Engineering: The New Corporate Espionage

What is Social Engineering?

Political definition:

- **Social engineering** is a discipline in social science that refers to efforts to influence popular attitudes and social behaviors on a large scale, whether by governments or private groups. In the political arena, the counterpart of social engineering is political engineering.

- For various reasons, the term has been imbued with negative connotations. However, virtually all law and governance has the effect of seeking to change behavior and could be considered "social engineering" to some extent. Prohibitions on murder, rape, suicide and littering are all policies aimed at discouraging undesirable behaviors. In British and Canadian jurisprudence, changing public attitudes about behaviour is accepted as one of the key functions of laws prohibiting it. Governments also influence behavior more subtly through incentives and disincentives built into economic policy and tax policy, for instance, and have done so for centuries.

Source: Wikipedia

Security Definition:

- **Social engineering**, in the context of security, is understood to mean the art of manipulating people into performing actions or divulging confidential information. While it is similar to a confidence trick or simple fraud, it is typically trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victims.

Source: Wikipedia

The Art of Manipulation

- Negative Connotations
- Is getting what you want manipulative?
- Some call it negotiation

- Learning to lie….or……lying well

Everybody Lies

American Psychological Association states people lie 13 times a day

Game of Deception: 2 truths & 1 lie

Step 1 in the game of elicitation.

Write down two things that are truthful about yourself and one thing that is a lie.

1. ____
____
____
2. ____
____
____
3. ____
____
____

Your online inventory

List all of the social networking sites you belong to

____
____
____
____
____
____

Please list the sites you are no longer active on

____
____
____
____
____

Which email address do you use to gain access to each of your social networking sites. Please list:

____
____

____
____
____
____

Do you use any of the same passwords on your social networking sites and your personal accounts?

____
____
____
____

Do your social networking sites disclose your birthday? _________________________________
Do your social networking sites disclose names of family members? ______________________
Do you social networking sites disclose your educational background? ___________________
Do your social networking sites disclose names of co-workers? __________________________
If no, would it be easy to find out? ____
Would your social networking site disclose what kind of vehicle you drive? _________________
Do your social networking sites reveal your political views? _____________________________
Do your social networking sites reveal where you have been on vacation? __________________
Do your social networking sites reveal associations you belong to? _______________________

Types of Social Engineers

Hackers

____
____

Penetration Testers

____
____

Spies

____
____

Identity Thieves

____
____

Disgruntled Employees

____
____

Disgruntled Customers

____
____

Information Brokers

____

____

Scam Artists

____

____

Executive Recruiters

____

____

Sales People

____

____

Governments

____

____

People in General

____

____

Information Gathering

Information gathering is necessary in all professions. Yet when it comes to an investigation, many individuals feel pressure gathering information. It is the most crucial component to the success of any Social Engineer.

Why do we gather information?

- To gain knowledge
- To gain clarity of a situation
- To resolve an issue or conflict

Why does the social engineer gather information?

- To gain knowledge

- To learn where the weakest links are in an organization
- To manipulate information in order to reach his or her goal

There are several different ways to gain access to information from a company. Some options include:

- Telephone
- Social media
- Dumpster Diving
- Tailgating

Information sources are only limited by the relevancy of the information they provide. When conducting research for social engineering, you may find yourself reviewing a broad range of sources (traditional and non-traditional) in order to gain a small bit of intelligence from each source. These bits are like puzzle pieces. Individually they don't look like much but when they're combined a larger, more coherent picture emerges.

Most Common Types of Social Engineering

- Phishing
- Telephone Solicitation
- Tailgating
- Shoulder Surfing
- Elicitation
- Social Media

Phishing

- Phishing is a criminal mechanism employing both *social engineering and technical subterfuge to steal consumers'* personal identity data and financial account credentials. Social engineering schemes use spoofed e----mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit websites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant crime ware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords -------- and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher----controlled proxies used to monitor and intercept consumers' keystrokes).

____

____

____

Tailgating and Piggybacking

- To describe the act of an unauthorized person who follows someone to a restricted area *without* the consent of the authorized person, the term **tailgating** is also used. "Tailgating" implies without consent (similar to a car tailgating another vehicle on the freeway), while piggybacking usually implies consent of the authorized person.

____

____

____

Impersonation

- **Crime**: As part of a criminal act such as identity theft. This is usually where the criminal is trying to assume the identity of another, in order to commit fraud, such as accessing confidential information, or to gain property not belonging to them. Also known as social engineering and impostors.

____

____

____

Shoulder Surfing

- In computer security, **shoulder surfing** refers to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and similar data.

____

____

____

Elicitation

- In the spy trade, **elicitation** is the term applied to subtle extraction of information during an apparently normal and innocent conversation. Most intelligence operatives are well trained to take advantage of professional or social opportunities to interact with persons who have access to classified or other protected information.

____

____

____

Telephone

- The **telephone** provides an anonymous (to a point) way of obtaining information. The drawback to using the telephone is caller ID and tracing. Social Engineers need to blend in with their environment to be successful. A simple phone call can reveal the company's name, the name of the person who answered the phone and so much more. After that phone call is completed, the social engineer can phone back and use the information obtained previously to obtain even more information.

____
____
____

Part II
Social Media

Risk: Corporate & Personal Brand

How many of us use social media & what platforms? Twitter, Facebook, LinkedIn, Instagram

What is the brand? ____

Greatest risk from social media is reputation

What can go wrong? What horror stories have you heard or experienced in regard to social media

- What are people saying about the corporation/brand
- Who is responsible for a response?
- Are employees commenting about the organization on social media? If they are they you're your unofficial spokespersons
- Who is in charge of crisis management & what defines the crisis?
- Disclaimers don't matter

Social Networking

- Type in a name of a co-worker or friend and see how many hits or matches appear with their information. Google, Facebook, Twitter, LinkedIn and others help people get connected, but they also help social engineers collect information about individuals, their families and their organizations. Social Engineering can be purely psychological, using information gathered about a person to obtain more information.

____
____
____

List 5 areas where your organization can be at risk

1.____
2. ____
3.____
4.____
5.____

Users of Social Media

Charlene Li & Josh Bernoff published a study called Social Technographics Report
They stated there are 6 types of social media users:

- Creators
- Critics
- Collectors
- Joiners
- Spectators
- Inactives

Group discussion

If it was your job to evaluate risk of social media risk what would you do?

____
____
____

How would you begin?

____
____
____

Does your organization have a Social Media Policy?

____
____
____

In your opinion is it comprehensive?

____
____
____

Does it clearly outline what the issues are or is it vague?

____
____
____

Does it clearly define what the consequences are for infractions?

____

____

____

How do you make staff understand the consequences?

____

____

____

If our privacy is desensitized by online communities, can we make people aware of what they do?

____

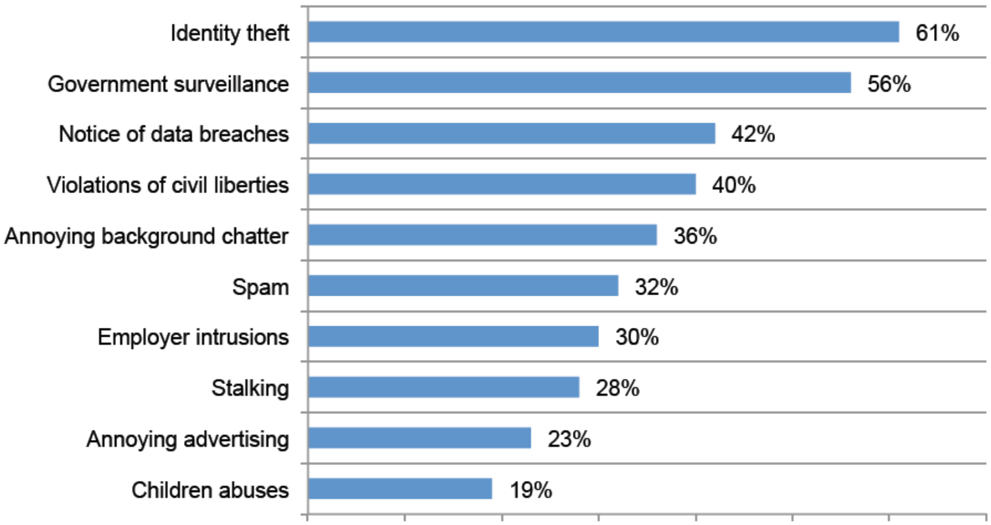
____

____

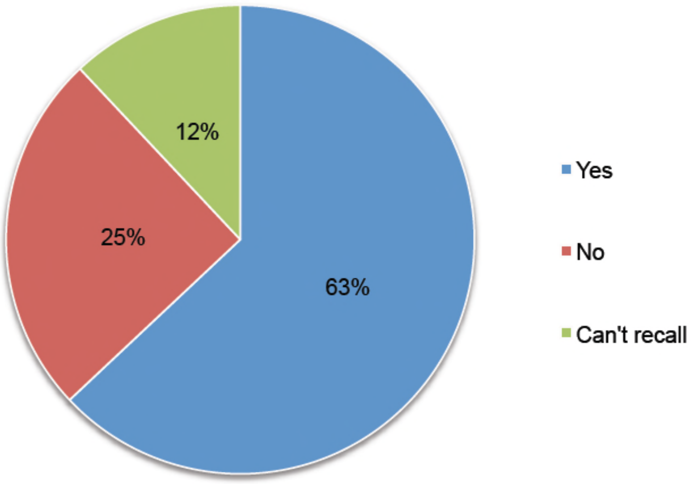
Privacy – www.ponemon.org

The Ponemon Institute tracks information regarding privacy breaches both from a corporate and individual perspective.

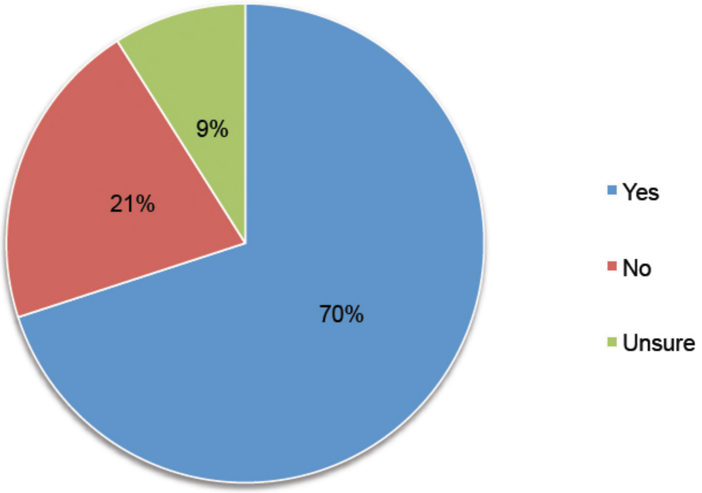
Bar Chart 3: What consumers consider the most significant privacy-related threats
More than one response permitted



Pie Chart 2: Did you ever share your sensitive personal information with an organization you do not know or trust?



Pie Chart 5: Did data breach notification cause you to lose trust in the privacy practices of the organization reporting the incident?



BUILDING POLICIES

Must Include:

- Clear instructions that provide guidelines for employee behavior for safeguarding information.

- Must be a fundamental building block in developing controls to counter potential security threats.

Biggest Roadblocks

- Perceived privacy infringements
- No one wants to be the bad guy
- HR won't like it
- Management doesn't think it is necessary
- In some ways it is no different than implementing internal fraud policies.

Controls that need to be in place include:

Social Media Policy

- Internal & external
- Who monitors it?
- What are 3rd party vendors saying and is that risk managed?
- Reputation disaster recovery – Who looks after it? Are they efficient?
- Are people trained to respond to negative posts? How?

Appendix I

Volvo Car Corporation's Policy for Social Media

This concerns the basics in the policy and the guidelines for Volvo Car Corporation and its subsidiaries within social media. The guidelines are directed towards anyone within Volvo Car Corporation who is blogging, twittering, producing and/or publishing pod radio or online videos or in any other way is present and active in different social communities and social media services.

Volvo Car Corporation in Social Media

Social media is a complement to all other traditional media and communications. Social media is built on communication and not only on information. For Volvo Car Corporation the usage of social media is a tool for increasing customer satisfaction as well as the possibility to sell more cars.

Key attributes for social media:
Listening
Engagement
Presence and participation
Creating a buzz and building relationships
Relevance
Receptivity and transparency
Consistency

Achievements
By participation in social media we can use our resources effectively and reach out to a large number of people, regardless of time and place. Our customers can be sure we are trustworthy, we care and react.

We can build our brand by participation in discussions, by connecting people and communities. By sharing corporate statements and by participation in discussions where brand and brand values are discussed.

Volvo Car Corporation has no views on employees' private lives or the thoughts or opinions that the individual employee may wish to share online. In order to aid online communication and avoid the risk of mistakes, Volvo Car Corporation has compiled a few guidelines along with tips and advice for people who are active in the social media and who therefore come up against issues that in some way affect the company.

Social Media Guidelines for Employees

Some online essentials
The guidelines, Code of Conduct and Brand Values that Volvo Car Corporation represent are all valid online as well as in real life.

- Be personal without getting private.
- Be open, link and refer to other blog comments for instance.

- Make sure you do not reveal any business sensitive secrets, launch of coming products or similar.
- Treat competitors with respect.
- Volvo Car Corporation Public Affairs does not moderate comments from employees.
- Once you have read through the social media guidelines and Volvo Car Corporation's Code of Conduct we trust that you will respect these and use your common sense.
- An employee at Volvo Car Corporation should not comment on legal issues concerning the company unless it is within their Volvo Car Corporation assignment.
- Always refer to the source.
- If there are any uncertainties you can always ask your manager or Public Affairs for guidance.

1. Responsibility.
The company understands and encourages those employees and associates who engage in online social media.

Volvo Car Corporation strongly recommends that you use your own name and that you are transparent with whom you represent when participating, sharing or writing in all online publishing. In online conversation, as well as in all other conversation, you are always an ambassador for the company even if you are not acting on behalf of the company. When you are acting privately, use your own private email-address (Gmail, Hotmail etc.). If you are acting as an appointed corporate spokesperson, you can use your corporate (xx@volvocars.com) email address.

If you are using social media for private purposes, use the same common sense as you would use for private phone calls, i.e. limit them to necessary activities and try to avoid such activities during working hours.

2. Honesty.
There are few things that make more impact than honesty. Therefore stick to the facts as you know them when you discuss topics related to Volvo Car Corporation and make sure they are within your area of responsibility. You should always make sure that you are not revealing any business sensitive information.

3. Privacy.
It is difficult to hold back when you get involved in a topic that interests you, but make sure to always protect yourself. Be careful with revealing any personal information about yourself and others. When something is published on the internet it will stay. The same goes for Volvo Car Corporation's secrecy obligation. The social media guidelines are subordinate to Volvo Car Corporation's Code of Conduct. Make sure you have read the Code of Conduct and that you respect the confidentiality and loyalty agreements between Volvo Car Corporation and you as an employee.

4. Disclaimer.
Make it obvious to others that your thoughts are your own and not the company's when you are acting on a private basis. There should not be any doubt as to who is the sender. This is important both from a purely legal point as well as from a point of trust. Marketing Volvo Car Corporation's products or disclosing information from Volvo Car Corporation, without letting people know that you are affiliated with Volvo Car Corporation, might harm your personal credibility.

5. Respect.
Today, posting, commenting or sharing is so easy that one can also easily miss the fundamentals in business and personal life. Laws still apply. Remember to validate the copyright if you post information that was not created by you. If you refer to information on other blogs, the common way of showing respect is by linking to the original post.

6. Be humble.
Respect is also about how you treat people. Always remain objective and treat people respectfully. Do not pick fights. Be the first to admit mistakes.

7. Protect.
Volvo Car Corporation's relationship with our customers, employees and partners is our most important asset, and it is important that we always protect this relationship. You cannot cite or disclose customer names without their approval. Protect your fellow workers and our customers, dealers, and vendors by refraining from sharing any of their personal information, statements, or photographs unless you have their written permission to do so. Bringing someone else into the conversation without their permission can be destructive to relationships, cause misunderstanding, or violate the law (including privacy and defamation laws), commercial contracts, or confidentiality agreements.

8. Competitors.
Writing about competition is good, but expressing negative thoughts about competitors without support of facts is not ok. If you write about competition, write with the respect they deserve as a competitor of Volvo Car Corporation.

9. Disagree.
It is ok to disagree with the opinions of others, but do so with respect.

10. Promote others.
Since we promote sharing and caring, Volvo Car Corporation believes that linking to other online actors is positive showing the source of information for example. If you find interesting information, provide links, generously.

11. If you need guidance.
Since Volvo Car Corporation believes in the best judgment of our employees, these guidelines are in the spirit of trust and openness. When in doubt, please ask your manager for advice. There are always consequences to what you publish. Therefore, make sure that you are comfortable with what you publish. As an employee you have a loyalty obligation towards Volvo Car Corporation, so be aware that what you publish may impact your employment. Concerning criticism against your employer or bad conditions at the workplace you should always discuss the issue internally with your manager or another company representative to enable corrective actions.

12. Whom to contact?
In the case of customer complaints or issues please make sure to forward these or advise the issuer to contact Volvo Car Corporation Global Customer Relations

Do not provide technical advice or post information related to vehicle modification or repair. Do not attempt to address customer product or service related concerns or complaints. Do not speculate regarding the cause or resolution of customers' vehicle concerns or complaints. Instead, inform the customer that you cannot handle the concern for them and that they should work directly with their dealer to resolve it. If the customer apparently has made a good faith effort to work with the dealer, refer the customer to the local Customer Relations Centre (or to the Global Customer Relations for redirection)

If you have questions about the company, you can also contact HR Service Centre

If a comment or question is outside your area of responsibility or beyond your level of knowledge so that an official company response is needed, bring it to the attention of a member of Public Affairs, Global Marketing or to the Legal department at Volvo Car Corporation.

13. Ideas and innovations.
Any questions or proposals such as new ideas or innovations should be sent to Intellectual Properties at Volvo Car Corporation. Abide by laws as you would in any other situation. This includes laws protecting intellectual property (such as copyright and trademarks), defamation, false advertising, competition (e.g. antitrust), and financial

disclosure laws. You should note that you may not use the Volvo trademark or other company brand trademarks on your personal sites.

YOUR EX IS YOUR GREATEST THREAT TO ONLINE PRIVACY

By Kelly Bourdet

With all the stories of Chinese hackers and unnavigable Facebook privacy settings in the news, people are rightly concerned about the security of their private information. But a new study conducted by McAfee anti-virus software–a brand that became famous during the 1992 Michelangelo computer virus scare, but has currently been in the news for the shenanigans of its long-departed bath salts-smoking founder--reveals that the greatest threat to your personal information is actually your significant other.

According to the study, 36 percent of Americans plan to send a romantic or sexy picture to their partner this Valentine's over text, email, or social media. Despite the ample evidence that current partners almost inevitably become ex-partners, and ex-partners aren't always the best guardians of our sensitive information, we continue to send scintillating texts and pictures with the naïve trust that we won't be exposed. Incredibly, this study found that about half of the people polled shared their passwords with their partners, which seems insane. Revealing their passwords opened them up to having personal info and personal pictures discovered and exposed by partners and ex-partners. McAfee compiled the rest of the results in a handy, very pink infographic.

Here at *Future Sex* I've covered stories on the consequence of partners hacking into phones and email accounts and I've also written a handy guide to sexting responsibly, if that's what you're wont to do. And although we've got to take McAfee's study with a grain of salt, it's essential truth – that men and women idealize both their partners and relationships in totally unrealistic ways, then flippantly provide other humans with theoretically permanent, inherently sharable records of intimacy – is worth contemplating. With the lover's holiday just around the corner, will the possible repercussions of sexting hold anyone back from doing it? I doubt it.

Entire empires, notably IsAnybodyUp, have been built on idea that, given the platform, there are people who want to shame their exes publicly. Though women are pushing back -- a recent class-action lawsuit attempts to hold a revenge porn site responsible for providing this sort of platform – the legality of these sorts of enterprises has not yet been successfully disputed. The potential for anyone's private photos to be broadcast is certainly real. In the above sex and tech survey, approximately ten percent of people had been threatened with the exposure of sensitive materials by an ex-partner. The most common reasons people for sought this type of retribution were "lying," "cheating," and "breaking up with me." So if you think there's even a possibility you might ever break up with you current partner, and you don't want to be naked on the internet, then it's probably best to resist the urge to share a picture of your naked body with someone.

Ownership of digital communication is not well established. You may "own" the copyright to any image you take, but this justification is essentially worthless when it comes to preventing an unwanted image from making the internet rounds. We've not yet established a way to hold anyone responsible for the damage that results from publication of these types of images, and it's an amorphous damage difficult to calculate.

Since the threat of exposure isn't stopping us from sharing risqué images, and sites that host revenge pornography continue to proliferate, it seems the ultimate result will be the reduction of shame around nudity. It seems unlikely that there will be, in the near future, a way to control the spread of unwanted images on the internet. What can legitimately ruin someone's career today can't possible retain the same level of injury as it becomes more and more common. Maybe the future is a place where a topless image of a woman on the internet becomes almost commonplace. In some ways, I think this is an encouraging future.

There are two distinct reasons that revenge porn is so disturbing. First, it's because of the betrayal of trust; no one wants their ex to lash out at them in this way. But perhaps more importantly, it is the threat of exposure and the consequences to our reputation that we fear. Maybe the most helpful move we can make regarding ex-partners sharing intimate stuff isn't to warn men and women everywhere not to sext – this won't work – but instead to not get so worked up about the image of a naked man or woman. So send a sexy picture if you want to, just realize you might be seeing it again somewhere unexpected.

FOR MORE INFORMATION CONTACT

Nejolla Korris

Nkorris@interveritas.com

www.interveritas.com

Subscribe to Nejolla' s newsletter at www.interveritas.com

Telephone: 780 457 6900