September 22, 2022

Taking Cybersecurity Seriously: Ten New Principles

By: Jack Hoskins

Legislation Commented On: Bill C-26 - *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 44th Parl, 2022.

Welcome to the golden age of cybercrime. An old pastime of mischievous young computer geeks is now the domain of nation states and professional hacker groups. It's a trillion-dollar industry. Attacks grow in number and scale every year and no one is safe, not even cybersecurity companies and the NSA. Tools developed to guard against cyberattacks are stolen and repurposed to make hacking faster and subtler. The worst is yet to come. Quantum computing may soon overpower all known methods of encryption, ushering in the "quantum apocalypse." Deepfakes and AI are only in their infancy.

It didn't have to be this way. For too long we have ignored endemic vulnerabilities in IT infrastructure that were less serious when developers significantly outpaced hackers in sophistication and tools. Times have changed. In this post I will explain the modern cybersecurity predicament in more detail and offer ten principles for how organizations can survive it and how we can hold them accountable. First, I will examine the theoretical basis of my principles. Next, I will examine the problem of cybersecurity law in a changing threat landscape. After that, the principles are presented. In the conclusion, I will make the case that these principles should inform the legal standards for cyber preparedness.

Normal Accidents and High Reliability Organizations

In 1984, Charles Perrow published the landmark book, *Normal Accidents: Living with High-Risk Technologies*, a study of accidents in complex, high-tech organizations with catastrophic potential. Perrow's argument, now known as Normal Accident theory (NAT), is simple: the higher the degree of *interactive complexity* and *tight coupling*, the more likely a system is to suffer from unpredictable "system accidents." These accidents are *normal* as in *inevitable*.

Interactive complexity means the degree of interrelationships between components of a system, be it an organization, a technological system or both. *Tight coupling* means the variety of causal interdependencies between two or more components in a system. Think of it as slickness. How easy is it to control component B if you control component A? Interactive complexity means that an accident can spread from one component to another, far away – often via a very short path; tight coupling makes this spread faster and easier.

What does all this have to do with hacking? Malware spreads far more easily in interactively complex and tightly coupled systems. Perrow would agree. The best illustration of this point is that hackers stole 10 GB of data from a Las Vegas casino after gaining access to the system through a fish tank thermometer.

Many scholars took issue with Perrow's theory. They believed that the risks he described could be overcome if the system was managed correctly – if it was a High-Reliability Organization (HRO). Many criteria have been advanced for what constitutes an HRO, including:

1. Extreme hierarchical differentiation.
2. Large numbers of decision makers in complex communication networks.
3. Higher level of accountability than in most organizations.
4. Higher frequency of immediate feedback about decisions.
5. Compressed time factors.
6. Multiple critical outcomes that must occur simultaneously.

The debate between the two theories is unresolved. Note, however, a subtle difference in scope. An HRO is first and foremost an *organization*, run by people. But interactive complexity and tight coupling can occur in systems *with or without* human involvement. If we accepted both theories, we would infer that automated complex systems are more dangerous, all else being equal, than systems with a human element. Furthermore, automation is not all-or-nothing: the less human involvement in a system, the riskier it is.

The ten principles listed below draw from these insights. But first, we must consider the ways in which the growth in cybercrime strains the capacity of regulation.

PIPA and *PIPEDA*

The rising frequency and severity of cyberattacks places a strain on any cybersecurity legislation that attempts to set a coherent standard for data protection. To understand why, let us examine three pieces of cybersecurity legislation. Two of them already apply in Alberta and the third, Bill C-26, is following on the horizon.

Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5 (*PIPA*) briefly addresses cybersecurity:

> 34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

The Privacy Commissioner tends to interpret this section as calling for evidence of a common-sense procedure for protecting data from breaches as sufficient (see *Little A Accounting (Re)*, 2022 CanLII 20313 (AB OIPC)). The Commissioner spends little time analyzing the merits of the procedure; so long as it meets a basic threshold of rationality then the organization is compliant with section 34.

Federally, the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (*PIPEDA*) includes the following provisions for cybersecurity:

> 4.7
> Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
>
> 4.7.1
>
> The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.
>
> 4.7.2
>
> The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.
>
> 4.7.3
>
> The methods of protection should include
>
> (a) physical measures, for example, locked filing cabinets and restricted access to offices;
>
> (b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
>
> (c) technological measures, for example, the use of passwords and encryption.
>
> 4.7.4
>
> Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information. (*Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96, ss 4.7 – 4.7.4, being Schedule 1 to the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.)

The principles in *PIPA* and *PIPEDA* are simple and common-sense. They are not biased toward any particular theory of cyber threat mitigation, nor are they onerously strict or precise. They reflect a wise deference to the specialized knowledge of engineers, programmers, and other cybersecurity personnel. *PIPEDA*, especially, is admirably thorough without being heavy-handed. In this climate, however, these rules risk becoming dated. As hackers become more sophisticated, security measures that would satisfy *PIPA* and *PIPEDA* are less and less effective.

One of three consequences will ensue: (1) the data protection portions of these statutes will be irrelevant to the vast majority of data breaches; or (2) the Privacy Commissioner will develop a bias towards ruling data holders noncompliant based on hindsight; or (3) a robust case law will develop around PIPEDA, applying intelligent standards of safety never contemplated in the statute itself. The Privacy Commissioner's concern with network segregation is a promising step toward legal recognition of the dangers of tight coupling, but more must be done.

Option (1) would be fine if there was nothing more that data holders could do about breaches. But there is. When cyberattacks are becoming more effective by the day, those who design and preside over complex IT systems need to be held to a higher standard. We are still trying to determine what this standard might be. The ten principles listed in the final section will offer some ideas.

Option (2) is problematic because it would leave *PIPA* and *PIPEDA* untethered to any coherent and fair standard for precautions.

Option (3) requires new principles for cybersecurity to guide the development of *PIPEDA* interpretation. We will discuss these principles after a brief consideration of Bill C-26.

Bill C-26

While Bill C-26 is too complex for an extended analysis here, two features deserve attention. First, the bill amends the *Telecommunications Act*, SC 1993, c 38 to establish greater cybersecurity protection.

Section 1(2) gives the Minister of Industry the power to issue an Order to a telecommunications provider compelling or forbidding one of twelve different actions. Such an order can bar a provider from upgrading a specific product or service, or compel the provider to "implement specified standards in relation to its telecommunications services, telecommunications networks or telecommunications facilities," among other things.

The second noteworthy feature of the bill is that it includes a new statute, the *Critical Cyber Systems Protection Act*. This Act specifically focuses on critical infrastructure such as pipelines and nuclear power. Accordingly, it gives regulators far more control over the cybersecurity of these systems than *PIPEDA* or *PIPA* provide. Here are a few examples.

Section 16 lets the regulator of a specific organization provide confidential information about that organization's cybersecurity plan to the Communications Security Establishment for consultation. Section 20(1) gives the Governor in Council the power to "direct any designated operator or class of operators to comply with any measure set out in the direction for the purpose of protecting a critical cyber system."

It is unclear whether government authority to direct specific cybersecurity measures will make critical infrastructure safer. This new strategy seems to rely on one or more assumptions: (1) the public sector takes cybersecurity more seriously than the private sector; (2) the public sector has a better understanding of cybersecurity than the private sector; or (3) the private sector has insufficient incentive to protect critical infrastructure from cyberthreats. It is easy to understand why regulators might operate under assumptions like these. Cyberthreats, like climate catastrophes, are becoming more frequent and severe, and it doesn't seem like cybersecurity and IT experts are doing much to stop it. However, a cursory look at famous public sector cybersecurity breaches suggests that government IT systems are not faring much better.

I believe that the problem is older and more fundamental than regulators and most IT professionals recognize. It cannot be resolved by stricter regulation because it is baked into the foundations of the interconnected, lighting-fast modern IT systems that we have spent the last thirty years perfecting. Simply put, our world is too efficient. The toxic byproducts of this pursuit of speed are turncoat technology, tremendous interactive complexity and tight coupling. As a result, new vulnerabilities appear regularly in even the most sophisticated IT systems. The stewards of the system must race against an ever-growing army of hackers to detect them. If the attackers win and breach the system, suddenly efficiency is not such a good thing.

What can be done? It is not easy to answer that question with concrete, tangible recommendations given the magnitude of the problem. Below, in the form of ten principles, is my attempt. Principles 1-4 are 'first principles.' Cybersecurity will never be optimized without keeping them in mind. Principles 5-10 discuss potential approaches to the problem.

Ten New Principles for Cybersecurity

1. Tools are turncoats. Machines have no loyalty. We have engineered loyalty in the form of locks, alarms, traps, passwords, private keys, firewalls, etc., but these tacked-on fixes can be circumvented with increasing ease. The Internet is uniquely antithetical to loyalty. We will not solve this problem by designing a new loyalty mechanism. It will inevitably betray us.

2. It is easier to break into things than to secure them. To be truly secure, a system must have no vulnerabilities. To break into a system, attackers only need a few. Because tools are turncoats, it is increasingly difficult to overwhelm attackers with superior technology.

3. Ambition breeds vulnerability. When the scale and ambition of a technological system increase, so does its complexity - including its interactive complexity. Normal Accident theorists tend to focus on our most ambitious technological feats – nuclear power, air and space travel, etc. Large-scale, complex projects are simply more vulnerable to unintended accidents than their simpler counterparts. Adding speed and efficiency only compound the problem by requiring tighter coupling and yet more complexity.

4. Efficiency and security conflict. You cannot have the safest computer system and the most efficient. Confidentiality and integrity cannot coexist with availability. This is well-known in IT circles, but many still think they can outsmart it and escape its implications. They can't. Efficiency and security will never be "complementary" or work together. If you can turn on a pump with the click of a mouse miles away, an attacker can do it from across the planet. The user's efficiency is the attacker's efficiency.

5. Our technologies are too efficient. We have erred on the side of efficiency. Until recently, engineers and software developers significantly outpaced hackers in sophistication. The risks of

chasing hyper-efficiency were muted. Only now has the chicken come to roost. But correcting this bias toward efficiency will not be popular with consumers who have long associated slickness and user friendliness with quality.

6. Break things up. Tight coupling and interactive complexity are liabilities. Instead of storing all of your data in one location, consider spreading it out among many. Instead of only using software and devices from one provider, use several. Modular systems are safer than integrated ones. Don't allow important devices to be controlled remotely. Try to break up your IT system into different segments connected by human intermediaries and paper. Reduce interoperability.

7. Take things offline. If a machine isn't connected to the Internet (and there is nothing a hacker can do remotely to establish a connection) then it is a lot harder to attack. Pipelines, water treatment devices and other critical infrastructure should be connected to the Internet as minimally as possible. Efficiency is not worth the risk.

8. Put people in charge. Automation breeds accidents. The fewer eyes on the system, the more problems fester undetected. Spend the time training people to understand the complexities your systems. Make them work with as few electronic intermediaries as possible – in other words, not from home.

9. Pare down. Interactive complexity increases exponentially when a new component is added to an IT system. It is impossible to predict every way that it may interact with other components. Add as few as you can get away with.

10. Strike a balance. How much speed and efficiency are you willing to give up for increased safety? Put a dollar value on it. Put a dollar value on what you stand to lose from data breaches. Do not assume they won't happen because they haven't happened. The factors listed above should be included, if they are not already, in risk assessments.

A Final Note on Law and Policy

The advantage of these principles is that they are non-technical. While measuring their implementation will be difficult in some contexts, it is not hard for someone without a background in IT to grasp them. If they have any merit, then they can improve the ability of the public (judges, commissioners and lawmakers included) to assess the quality of cybersecurity measures. This in turn could increase the accountability of IT professionals and anyone presiding over a networked organization. That, along with encouraging a more sober and effective approach to cybersecurity, is my goal. A lot of trial and error must happen before we achieve these aims. If the principles above are of no use, then others must be found. Cybersecurity and cybersecurity law share a common fate: if the stewards of IT systems cannot protect them, then regulation can only help with the cleanup.

This post may be cited as: Jack Hoskins, “Taking Cybersecurity Seriously: Ten New Principles” (September 22, 2022), online: ABlawg, http://ablawg.ca/wp-content/uploads/2022/09/Blog_JH_Alberta_Cybersecurity.pdf