Toward More Secure Networks
For Critical Sectors

Remarks to
The ABA Standing Committee on Law & National Security

By Joel Brenner
Senior Research Fellow
Massachusetts Institute of Technology

The University Club of Washington, DC
October 18, 2017

• ACKNOWLEDGMENTS AND GREETINGS

I’m going to do two things this morning. First, I’ll report to you on work we’ve been doing at MIT on protecting critical infrastructure networks. The strategic point I will leave you with is that the principal obstacles to greater security are not technological; they’re legal, commercial, and political. Second, I’m going to make the case that the legal component of this challenge should be a core concern of our Committee.

Unless you’ve been living under a rock, you’re aware that critical social functions are under attack. Some examples:

➢ Saudi Aramco, Ras Gas (2012) (Iran) – payback for Stuxnet
➢ Seoul Banks (2013) (DPRK)
➢ The Ukrainian electric grid (2016) (Russia)
➢ Dyn (2016) (Internet services unavailable in Europe and North America)
➢ The British National Health Service (2017) (DPRK)
Especially worrisome is that criminal organizations as well as foreign security services and their cut-outs now have the prowess to launch this kind of attack. You remember ransom-ware attacks on hospitals. Imagine a ransom-ware attack on a regional transport network.

The digital systems that control critical infrastructure in the United States and most other countries are easily penetrated and architecturally weak, and we’ve known it for a long time. Since 1990, however, Presidential leadership on infrastructure security has been hesitant and chiefly rhetorical. President Trump’s recent executive order clearly intends to change that, but the proof will be in the follow through, and we should watch closely for next steps. Meanwhile, system operators and policy proposals have tended to focus on short-term fixes and tactical improvements, such as marginally better tools for attack discovery and response, setting up security operations centers where none existed, information sharing (usually in the form of complaints about the government rather than fostering intra-sector sharing among firms), and of course, more and better training. These are well and good. Smart people in and out of government have been working hard at them, and they’re important. But they are purely tactical adjustments. We’ve been saying and doing these things for fifteen years, as all the while we’ve been walking backwards on network security.

This is a losing game. Most critical infrastructure is less secure now than it was fifteen years ago. (Not because we haven’t become better at defense; we have. But the offense has also gotten better, and the threat environment is worse.)

Much effort has also been devoted to developing better security standards, but most standards are merely advisory, and there are too many
of them. In any case, compliance does not imply security – a fact that continues to baffle many board rooms. Heartland Payments systems and Target were compliant with payment card industry standards when they lost huge volumes of customer data. Without compliance, a firm is most unlikely to become secure – but compliance is merely a baseline.

Meanwhile, key federal departments, notably but not exclusively homeland security, defense, and energy, have worked hard to encourage better infrastructure security. But these efforts have not altered, and cannot alter, the dismal strategic balance in which the defense holds the short end of the stick, and in which weak nations, and eventually non-nation-state actors, can harm the United States at painful levels that are intentionally below the level of armed conflict.

At the same time, the vulnerability of this infrastructure is a constraint on America’s freedom of action in the world – even at the military level. For instance, following the attack on JP Morgan in 2014 – initially thought to come from Russia – the New York Times ran a story based on a leaked account of a meeting where President Obama asked his intel chiefs whether Putin was sending him a message. He wanted to know whether Putin was signaling that if we expanded our role in Ukraine, Russia would take down a U.S. bank. Henceforth, no President can make decisions about force projection without taking private sector vulnerabilities into account.

The underlying problem is that the owners and operators of critical infrastructure have aggressively aggregated data and linked functions without regard to long-term risk. They have also retrofitted industrial operating technology with digitized controls exposed to the Internet. The control for a railroad track switch, for example, or a power generation plant,
used to be locked up. They’re now reachable and potentially controllable electronically from many places on earth. The efficiencies such linkage created for managing distributed technologies were immediate and obvious. The vulnerabilities were also immediate, but they weren’t obvious to people who weren’t computer geeks – or they were deniable. They’re now obvious to everybody, and they’re no longer deniable.

About two years ago, several of us at MIT began asking what would a substantially more secure network environment for critical infrastructure look like? And what prevents our getting there? To answer these questions, we convened workshops to explore four critical verticals: electricity, communications, finance, and oil-and-gas. We limited sessions to twenty participants: half from prominent businesses and the rest from academia and government. And we imposed the Chatham House Rule: No quotation, no attribution. We wanted a candid conversation, not prepared presentations. We simply asked participants to describe (1) the greatest strategic risks they faced, and (2) the most important challenges that would help diminish those risks.

The resulting report, published in March, distills the results. It covers a lot of ground, but in the brief time I have this morning, let me talk only three of our recommendations:

First: We proposed that key operating controls be isolated from public networks if they were to be made reasonably secure – not all controls, but rather those controls on the very few functions that must not be allowed to fail. Of course, saying this is the beginning, not the end, of a conversation. There are reasoned differences of opinion about what “isolation” means, and about appropriate degrees of isolation, and about how to accomplish it. But the idea is realistic. For example, I know of a pipeline operator that runs
parallel pressure controls on its line. If its digital controls were corrupted to permit the pressure in the line to rise dangerously and trigger an explosion, a separate, isolated control would automatically shut the system down. That control would literally be invisible from the network. Many businesses will resist this kind of thinking because it will cost money, either in equipment or labor or both. But security must be paid for.

Second, our government, together with like-minded governments, should support a market for simpler, safer control technology. Why? Because complexity is the enemy of security. Superfluous functionality brings with it multiple vulnerabilities. Yet controls are marketed for many purposes, and the chips in those controls are field programmable gate arrays. FPGAs are cheap precisely because they can be used for almost any purpose. Which is why the chip in the control on a pipeline valve – all it does is open and close the valve – could be the same chip that’s in your kid’s game box. Malicious code is easy to insert among two million lines of code, and may be impossible to find. Participants in our oil-and-gas workshop were adamant about this, stating flatly that existing controls represent a supply chain vulnerability they understand but are helpless to alter. Fixing this will be a heavy lift.

Let me be clear: We have not proposed the invention of new technologies. That would be a non-starter. We do propose research into modifications to existing commercial technology. For example, could whole sectors in existing chips be reliably and verifiably rendered inaccessible, or useless, in order to limit functionality? I don’t know. The answer would presumably depend on the architecture of the chip. But it’s worth finding out. Assuming the answers to this and similar questions were promising, governments ought to support a market for simpler controls. DoD and DoE
should lead this effort. If the demand were there, the supply would be there. Implementing this recommendation has the potential to make it substantially more difficult to see, resist, and recover from attacks. However, acting on this recommendation would require vision, determination, and organization not yet evident in either Congress or the Executive Branch.

Third, four factors drive behavior in a market economy: (1) market opportunity, (2) tax policy, (3) liability, and (4) regulation. For the moment I will leave regulation aside and note that we have failed to employ tax policy as a security driver. Our report therefore recommends tax incentives to encourage the accelerated retirement of legacy systems. Participants in all our workshops felt this was a significant challenge.

I also note that our current liability regime is radically misaligned with security. I can’t think of any other area of our collective commercial life in which one can introduce unsafe or unsuitable goods with no liability for the economic consequences. Do you recall the DDOS attack on Dyn last year? It was orchestrated through a botnet comprising a million or so linked video security cameras, none of which had any security protection. The incident was one of several early inklings of the dystopian possibilities of the so-called Internet of Things. If the manufacturers of those cameras had faced third-party liability for the foreseeable consequences of marketing those devices, how many days would it have taken to pull those devices from retail shelves?

Now, allow me an observation. None of these three key conditions creating insecurity has a technological solution. The failure to deploy existing technology is not a technological problem.

➢ We know how to isolate networks.
➢ We know how to make simpler, safer chips and controls.
➢ We know how to create tax and liability incentives.

We also know how to create a more secure domain name system and border gateway protocols, but we don’t do it. This is why the MIT study concludes that the most difficult cybersecurity challenges are legal, commercial, and political – not technological.

It seems to me – I am not the first to say this – that we are at a juncture reminiscent of the debates about motor vehicle safety in the mid-1960s. In April 1966, the Seventh Circuit, in Evans v. General Motors, held that GM was not liable for the fatal consequences of a side-impact collision involving its “X” frame-chassis, which provided no protection against side-impact collisions. As the dissent described the holding, “The opinion of the court decides that General Motors' duty was, as it concedes, to design its automobile to be reasonably fit for the purpose for which it is made, and free from hidden defects; [but] that notwithstanding General Motors' foreseeability of possible broadside collisions, the "intended purpose" of the automobile does not include its participation in such collisions....”

Later that year Congress passed the Highway Safety Act and the National Traffic and Motor Vehicle Safety Act. That legislation changed the vehicle market and dramatically reduced traffic fatalities. Instead of only expecting drivers to modify their behavior, the act sought to change the safety environment by imposing duties on manufacturers and to alter the interaction between driver and vehicle. It seems to me we’re at a similar juncture, or should be. Bad driver behavior is indeed responsible for many accidents, just as online behavior is responsible for many cyber intrusions. Trying to improve behavior is worth the trouble, up to a point. Yet any regime that places security wholly in the hands of users is destined to fail,
because when security butts heads with convenience, convenience wins every time. Instead, we should be aiming to change the entire environment, and that includes the behavior of software manufacturers. In my opinion, this cannot be done without the imposition of a reasonable liability regime that is sensitive to innovation but intolerant of knowingly or recklessly insecure products. To those of you who are politically allergic both to regulation and to anything that might benefit the plaintiffs’ bar, I say this: Our only other alternative is the highly unsatisfactory status quo. These are our three choices – our only three choices – and it seems to me that the least intrusive alternative to the status quo is an evolving liability framework. The current legal order is undermining our nation’s security. It is also out of whack in principle for the following reasons:

1. It encourages the marketing of software known by its manufacturers to be insecure and, in some cases, knowingly unsuitable for the uses to which it will be put. Software is virtually always marketed in beta versions, even for critical uses, thereby facilitating the externalization of risk. Patching is a good example. Patching can never be automatic, even in firms committed to good security. A patch list is as long as your arm; firms must triage. Even then, to install a patch on a complex system without testing it first can crash the system. But testing is expensive and time-consuming, and the user bears the costs. (This may account for the rueful joke that only two kinds of businesses refer to their customers as users.)

2. In most cases, the lack of liability probably places the risk of failure on the parties least able to insure against it. It certainly removes the ability of insurance carriers to reduce risk by inducing their insureds
to improve software quality, because they’re insuring users rather than manufacturers. This is bad policy.

3. Lack of liability has moved us backward to a regime of *caveat emptor* – and it does so in an area where licensors, even in most large enterprises, are in no position to evaluate the quality of the goods and services on offer. This is irrational as well as unfair.

4. Treating software licenses as sales under Article II of the UCC denies licensees the rights ordinarily incident to a purchaser while giving manufacturers the benefit of warranty exclusions ordinarily incident to a sale. This is deeply unfair and can probably be fixed only by statute.

Fifteen years ago, an argument about liability for poor software would have sounded like a garden variety commercial dispute. I hope it’s clear by now that it is no such thing. Our entire world is dependent on reliable and reasonably secure software, and the lack of it makes it increasingly difficult to protect the nation’s vital functions: power, communications, transportation, and finance, to name a few. The question of software liability is therefore a question of law and national security, and is thus tailor made for the attention the ABA’s Standing Committee of that very name.

Thank you.
Change agents:
FTC’s investigation of Equifax
European courts and regulators
- Kingsway Hall Hotel Ltd v. Red Sky IT (Hounslow) Ltd, High Court, Q.B. Div., May 2010, holding that a commercial software system “was not fit for the purpose for which it was sold” and “did not meet the standard that a reasonable person would regard as satisfactory.”

Coordination of Research Policy
- Corporate and government research budgets should focus on the identified research challenges.
- Here are four research challenges:
  Research Challenge (1)
  Quantify Network Risk
  - The inability to quantify network risk impedes investment in cybersecurity.
  - Varied elements of risk (network fragility, external threat, and internal behavior) make measurement difficult.
  - Can insurance carriers measure risk indirectly by loss experience?
  Research Challenge (2)
  Automate Detection and Response
  - Attacks have been automated. Defenses must also be automated and must be capable of learning and adapting. This is a true technological challenge.
  - Major concern: a slow-moving strategic attack on the financial sector that corrupted data rather than shut down systems. Could we detect it before it corrupted back-ups?
  Research Challenge (3)
  Cross-Sector Disaster Simulations
  - Where is the data needed for a sophisticated simulation of a cyber disaster? Who will share it?
  - New MIT project to enlist cooperation based on the secure storage and use of anonymized, encrypted data.
  Research Challenge (4)
  The Internet of Things
  - The IoT makes attack surface management geometrically more difficult. We saw the consequences in the Dyn attack.
  - Should enhanced security be applied at the device level or only at higher levels within networks?
What liability should attach to makers/sellers of insecure