Cybersecurity Breaches: Causes, Consequences, and Countermeasures

Josephine Wolff, The Fletcher School at Tufts University

Published on 1st February 2021

Michael Klein:

I'm Michael Klein, executive editor of EconoFact, a non-partisan web-based publication of The Fletcher School at Tufts University. At EconoFact, we bring key facts and incisive analysis to the national debate on economic and social policies, publishing work from leading economists across the country. You can learn more about us and see our work at www.econofact.org.

Michael Klein:

In December 2020, the Trump Administration acknowledge that hackers broke into key government networks, including those of the Treasury, State, Energy and Commerce departments. In this so-called SolarWinds attack, the hackers were acting on behalf of a foreign government, most likely Russia.

Michael Klein:

This looks to have been one of the largest and most sophisticated attacks on the federal system in the past five years. Of course, we have seen other examples of widespread cybersecurity breaches such as in 2013, when attackers stole over 40 million credit and debit account numbers, and personal information on an estimated 70 million customers from Target.

Michael Klein:

Are cybersecurity breaches something that can be stopped or at least limited? Or in our interconnected world, are businesses, governments and individuals just going to have to learn to live with them? And how costly are these attacks from an economic perspective, as well as from the perspective of national security and personal privacy?

Michael Klein:

To discuss these issues, I'm very pleased to be speaking with Josephine Wolff. Josephine is my colleague at The Fletcher School at Tufts University, where she is a professor of cybersecurity policy. She's also a columnist for the New York Times. Her 2018 MIT press book has the striking title, You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches.

Michael Klein:

Josephine, welcome to EconoFact Chats.

Josephine Wolff:

Thanks Michael.

Michael Klein:

Josephine, when we talk about cybersecurity breaches, I imagine this covers a wide range of different types of attacks on businesses, individuals and governments?

Josephine Wolff:

Absolutely. When we think about the different types of cybersecurity incidents out there, we often bucket them into a couple of different categories based on the motivation of the attackers. So there's a big bucket, which is most of the incidents and breaches hear about, which are financially motivated cyber crimes.

Josephine Wolff:

People who are trying to make money by installing ransomware that demands a Bitcoin or other cryptocurrency ransom from the victims, or stealing your credit card numbers or personal information so that they can steal your money. That's what we often call cybercrime. And then there's another category of attacks that we think of as the espionage attacks.

Josephine Wolff:

So either political espionage, where a foreign government or other group is trying to steal political or national security information. And another category of that, that we sometimes talk about is economic espionage, where a government or private entity may try to steal intellectual property or proprietary trade secrets from an industry victim.

Josephine Wolff:

And then finally we have a category that we sometimes call cyber sabotage. And that would be something like the 2011 Stuxnet worm that targeted the Iranian nuclear enrichment facilities, where you actually use computer code to try and sabotage some piece of physical infrastructure or operations, not to profit financially, not to steal secrets, but to actually execute some kind of operation.

Michael Klein:

Have we seen an increase in the sophistication of these three types of attacks, cyber crime, espionage and sabotage over the past decade?

Josephine Wolff:

I think we have, it's not a completely linear progression towards always more and more sophisticated attacks. But certainly the ones that we've seen that are really sophisticated including the recent SolarWinds compromise suggest that, these are adversaries who are becoming more technically talented, who are building up more capacity and better experts in this space and are able to deliver a lot of malicious code or malware in very subtle and very difficult to detect ways.

Michael Klein:

As you mentioned, the intense of these attacks are different depending upon, whether the hackers are part of a criminal network or working for or at the behest of a government. Do they tend to differ in their methods as well?

Josephine Wolff:

Somewhat. Certainly you see when people are working for or on behalf of a government, there's often a lot more willingness to do really expensive and time-intensive things, whether that's designing a piece of code specifically to target one particular system or exploiting what we call a zero-day, which is a vulnerability in a computer system that's never been exploited before.

Josephine Wolff:

And if you want to buy those, they're quite expensive so we often associate those with government sponsored attacks. Whereas when we see private entities or criminal networks operating on their own, they're usually thinking more about the bottom line. They're usually more focused on financial profit.

Josephine Wolff:

And so often you'll see them going after the easiest victims, the lowest hanging fruit, thinking more about how they can get the most mileage for the tools that they've already got.

Michael Klein:

What are the various types of costs to a business that suffers a cybersecurity breach or cyber crime?

Josephine Wolff:

It depends a lot on the type of attack and also on the type of business. If we think about something like ransomware, there's a very immediate direct cost for organizations that actually pay the ransom, there's that ransom. But there's also a number of less tangible costs involved, where you could think about the reputational costs that would be associated with having everybody know that your business had been breached.

Josephine Wolff:

They're the mitigation and clean up costs, which can be significant where you have to go in and replace a lot of your software and sometimes even your hardware. That Target stores breach that you mentioned, actually involved Target replacing for all of their payment card terminals. That was incredibly expensive as well.

Michael Klein:

And it's not just the company that's the target of the attack that's hurt, right?

Josephine Wolff:

Absolutely. One of the things that we worry about a lot in the field of cybersecurity policy is that, most of the people who are affected by large scale breaches of information are not the people who are in a position to protect it, are not the organizations that actually let it be stolen but are instead those organizations individual customers.

Josephine Wolff:

And those externalities, those people who have that negative impact, even though they don't have any control over the protection, are often the people we worry about most in the aftermath of these types of incidents, because the organizations don't necessarily have any strong incentives to protect their information better if the organizations aren't bearing the costs of losing them.

Michael Klein:

I'm glad that you used the word externality, as you know, that's a big concept in economics. So an analogy, it's a little bit like if I had a campfire in my backyard and the burning embers tended to be blown to my neighbor's house rather than mine, I won't spend enough time tending to the fire.

Michael Klein:

That standard problem of an externality where people don't bear the full cost for their actions or in this case, their inactions, is a problem that we see with cybersecurity?

Josephine Wolff:

Definitely. There's a big concern that organizations underinvest in cybersecurity because they look at the consequences and the costs of these incidents and breaches. And they say, "You know what? That seems less bad than having to spend millions of dollars protecting our data and our networks."

Josephine Wolff:

And part of the way they make that calculation is knowing that if there's some breach, there will be cost to them. They will have to pay to notify everybody who was affected, they may have to settle some class action lawsuits. But a lot of those costs, a lot of the actual identity theft or financial fraud is going to be born by the payment card networks or the individuals.

Michael Klein:

Continuing with my campfire example, people have fire insurance for their houses. Is there a market for insurance for cyber attacks?

Josephine Wolff:

Yes, there is. There's a pretty rapidly growing market for cyber insurance that we've seen increasing about 30% year-over-year in terms of principal payments. And it covers a whole range of different types of incidents, from data breaches, to ransomware, to denial of service attacks that actually take your computers offline and it's really growing quite remarkably right now.

Michael Klein:

Are we going to see that GEICO Gecko advertising cybersecurity insurance sometime soon you think?

Josephine Wolff:

I think the question of when it's going to reach the personal market is actually a really interesting one. And there are some firms that are already starting to experiment with that, mostly just with very high-net-worth individuals, but I don't think it's impossible.

Michael Klein:

Suppose that I did have cyber insurance or if I was heading a company, I had cyber insurance. Is there a problem that, if I have the insurance I might not pay enough attention to actually protecting myself or my network, the problem that economist called moral hazard?

Josephine Wolff:

Definitely. This is another big concern around the insurance space here is that, when insurers come in and they sell these cyber insurance policies, they often don't have a very clear sense of what the requirements should be for their policy holders in terms of their own security. So you think about, fire insurance and the things we all take for granted, we all have consensus are important, like smoke detectors and fire extinguishers, sprinklers.

Josephine Wolff:

And we don't know what the equivalent of smoke detectors for cyber security intrusions are. We don't actually have clear data or clear consensus on what are the five or 10 or 15 things that every firm should be doing. And it may be that there's not one set for every firm, it may be that there needs to be some variation.

Michael Klein:

I guess it looks like there are two issues here. One is that, technically it's very difficult and secondly, there are lots of sources of cyber attacks. So that multiplies the difficulty of having an insurance contract where you're either covering everything or demanding that the people insured take the proper steps?

Josephine Wolff:

Absolutely, those are both real problems.

Michael Klein:

When this happens, do insurers actually pay ransom, in a case of a malware or something? Is that something that we've seen the insurance companies do?

Josephine Wolff:

Yes, it is. We've seen local city governments in a couple of towns in Florida, ask their insurers to make ransom payments. We know we've seen it in other places in the private sector, much of it goes unreported because ransomware attacks aren't mandated to be reported under law. And so examples we know about are mostly in the public sector where like a city council had to vote on it.

Josephine Wolff:

But it's absolutely the case that insurers cover large portions sometimes up to hundreds of thousands of dollars of these ransom payments that are made directly to criminals. And that just makes it more profitable to launch ransomware attacks just encourages those criminals and other criminals to keep doing that.

Michael Klein:

Is there evidence that in fact these payments are encouraging others to make these attacks because it's profitable to do so?

Josephine Wolff:

Well, we do know that we've seen certain organizations targeted just because their insurers are advertising them as clients when they're describing their cyber insurance offerings, which suggests that yeah, they may actually be specifically targeted because the attackers know, "Oh! They've got insurance, they'll definitely just pay up because they're not even going to have to pay out-of-pocket."

Michael Klein:

I'd like to shift the focus a bit now to the SolarWinds cybersecurity breach that compromise the U S Treasury, State, Commerce and Energy departments among others. What was the nature of this most recent attack or at least an attack that we just learned about in December?

Josephine Wolff:

This is a really interesting and a really scary kind of attack for people who think about cybersecurity because the way the SolarWinds compromise happened is, the perpetrators didn't go directly after the networks of the departments in government that they were trying to get access to.

Josephine Wolff:

They instead first infiltrated a vendor, that's the SolarWinds company that sells software to many parts of the government as well as many customers.

Michael Klein:

What kind of software does SolarWinds sell?

Josephine Wolff:

The software that was involved in this is, a line of products called the Ryan that help companies monitor their network. It's security software, it's supposed to help you see what traffic is coming in, what's going on.

Michael Klein:

That's deeply ironic, isn't it?

Josephine Wolff:

Deeply ironic and even more ironic, the compromise happened through an update to that software. And you know how the security people like me are always saying, "Oh! You have to download all your updates, it's so important for security." Here's a case where that update was actually what compromised the entire system.

Michael Klein:

Yeah. I know you've told me to do that. Should I stop doing that now, Josephine?

Josephine Wolff:

Well, that's the fear, that everybody's going to read about SolarWinds and say, "Oh! These updates, they seem really dangerous because of how they were used in this case."

Michael Klein:

I imagine that attacks of this nature are really difficult to guard against?

Josephine Wolff:

Absolutely, right. When we think about, the range of different ways that we advise organizations to take stock of their networks and their data flows and try to protect them. One of the hardest, and we've known for a while very important pieces to that, but we haven't seen play out as dramatically.

Josephine Wolff:

What happens is if it fails is, how do you know all of the different companies that are providing you with software, that are providing you with online services are also secure in what they're doing? And if you have amazing security but those vendors are not secure, then your security doesn't matter at all because they already have access to your networks.

Josephine Wolff:

And so the things that we advise in this space, like keeping a comprehensive inventory of all of your vendors and doing an assessment or an audit of those vendors' security practices, are really time-intensive if you have as many vendors as say, the federal government does.

Michael Klein:

Going back to the campfire example it's like, you can't trust smoke detectors, so it's not that useful. And in fact, the smoke detectors themselves might spark and cause a conflagration?

Josephine Wolff:

Exactly.

Michael Klein:

So Josephine, you described the responsibility or the range of responsibility for the SolarWinds breach. Is there a similar range of responsibility for something like the breach of Target, where it's both the provider and the user who has to be held responsible and should have been stepping up more to take care of this?

Josephine Wolff:

Yeah, I think Target's a great example of this because Target is actually also a breach that happens through a third-party vendor. They have an HVAC provider who's doing the air conditioning and cooling in the stores, who has access to one of their online portals. And the attackers used that access from that HVAC vendor to get into the Target system and then steal all the credit card numbers for all of the Target customers.

Josephine Wolff:

And I think, again, you see exactly that same complicated liability story where on the one hand, the HVAC vendor should have done a better job of protecting those credentials and protecting that access. But on the other hand, Target should have been much more aware of what was going on, on its networks and who it had given access to.

Michael Klein:

This is demanding a level of coordination that might make it very difficult to actually prevent these in the future?

Josephine Wolff:

Yes, I think that's right. That if we're going to do a better job of preventing this type of attack, we need to have much clearer standards and expectations around how you're supposed to secure your supply chain and what that looks like.

Michael Klein:

What lies ahead Josephine, where do we go from here? Have there been any signs from say, the new administration on how they may act on these issues? It's only been a few weeks, but have they given any indication yet?

Josephine Wolff:

I would say, we don't have a very clear sense of what their cybersecurity priorities are going to be beyond perhaps a new data protection bill, which might deal with things like when companies have to report that they've been breached, when they have to announce to the world that some security incident has happened.

Josephine Wolff:

I think in terms of recovery from the SolarWinds compromise, probably what you're going to see is the Biden Administration try to do a very comprehensive overhaul of all of the computer systems and networks across the federal government to understand the scope and the scale of what's been compromised, and try to weed out all of the infiltrated systems and make sure that they're secure.

Josephine Wolff:

And then looking a little longer-term I think where we go from here is to thinking about, how do we address supply chain security or cyber risks in a more comprehensive and systematic way moving forward?

Michael Klein:

And do you see the private sector starting to respond more aggressively to these problems? Or is there the complacency because of the reasons that we discussed earlier?

Josephine Wolff:

I think you're going to see some entities in the private sector getting more aggressive. If we look at this latest SolarWinds compromise, we know Microsoft's been very heavily affected by it, we know FireEye was very effected by it. I think you're going to see companies that have really seen their security undermined in a major way, start thinking about it much more seriously.

Josephine Wolff:

I think for a lot of the smaller players though, those externalities and incentive problems are going to be an issue until there's some kind of policy or requirement.

Michael Klein:

What about, Josephine, at the individual level? What should I be responsible for? What am I liable for and so on?

Josephine Wolff:

I think that when we try to understand the individual responsibility around these types of incidents, it's pretty clear pretty quickly that a lot of the fault lies more with some of these systematic processes. But that once we've done a better job of trying to lock down some of those holes, then there is going to be an increasing amount of responsibility and liability for individuals who are downloading malware inadvertently.

Josephine Wolff:

And it's just that we haven't gotten to the point where the signals are clear enough, where it's straightforward for individuals to operate in this space that we can really hold them responsible when things go wrong. I'd say at the individual level, you're very responsible for your own devices and your

own accounts and thinking about, are you keeping the software updated? Are you paying attention to any warning signs or suspicious activity?

Josephine Wolff:

Are you using strong passwords and two-factor authentication? Because if your accounts or your devices are compromised, then they can be used to attack other people. You are probably not going to be liable for that in any legal sense, just because of how complicated these attacks are.

Josephine Wolff:

And the fact that many people's computers are compromised and used to attack other people, but you're still going to be responsible for doing your part in that larger ecosystem to help secure the larger internet.

Michael Klein:

All of this is a little bit scary, it's kind of a jungle out there. But I'm really glad that people like you are working on addressing these issues because they have a lot of importance at the economic level in terms of personal privacy and even national security. Thank you for taking the time to speak with me today, Josephine, about these important issues.

Josephine Wolff:

Thank you so much for having me.

Michael Klein:

This has been EconoFact Chats. To learn more about EconoFact and to see the work on our site, you can log into www.econofact.org. EconoFact is a publication of The Fletcher School at Tufts University. Thanks for listening.