

## IBM AND THE FUTURE OF DATA SECURITY

KNECHT: Welcome to the Economics of Security Webcast. I am joined here today by [Catherine Mann](#), who is a professor of international economics and finance at Brandeis International Business School. And Peter Evans, who is a director at IBM Internet Security Systems.

So today, Catherine, we want to start with you talking a little bit about some research that you've done recently related to the economics of security. Who holds the risk when major data breaches are occurring?

MANN: In some sense individuals are much less responsible for data breaches than is the enterprise. It makes sense because the enterprise is where the data are being collected and where the data are being kept.

And so if somebody wants to get at data, they're going to go to the place where they can get a lot in one fell swoop and that's not at the individual user, it's not at the individual points of transaction; it's at the enterprise level.

EVANS: Absolutely. What we're actually seeing is some enterprises adopting fairly innovative technologies, not only to harden their own core databases, their own core networks, but actually to create almost dissolvable agents that can reach out, protect the enterprise or protect the end user during the course of commerce being conducted but actually without putting the layers of complexity in front of that user. You know, people trade off convenience for security, and that's not a trade off that we want people to make.

KNECHT: So Catherine, are there certain ways or policies that you've seen are successful in helping businesses protect themselves from these kinds of breaches? And what would your recommendations be based on your findings?

MANN: Well, there are three approaches to dealing with creating an environment to improve the incentives for businesses to engage in the type of internal controls and consumer outreach that yields a much more secure environment for the transaction and for the data associated with their transactions.

The first strategy is of course having a government mandate that sort of tells consumers what to do and tells businesses what to do. That is where legislation can go.

The second strategy is internal peer review within the set of enterprises and the community itself and sort of acting on each other and sort of naming and sort of saying, shame on you, make sure you improve your operations, because you're making us all look bad.

And then the third approach is to have enhanced reputational consequences if an enterprise does not have appropriate degrees of security and experiences a data breach.

Now, where these three work together or have the potential to work together to be complementary in such a way as to enhance to incentives for businesses to employ

internal controls and to enhance the customer and experience is to have transparency when a breach occurs.

Now, that transparency enhances the financial loss to an enterprise that does not have controls. So any individual enterprise will not actually want to vote for more transparency because they're always afraid that they're going to be the one that all of a sudden shows up in the newspapers and they don't like that. But that is the only way in which the market can incentivize companies to improve internal controls.

EVANS: Some simple real world examples that we're seeing recently that are actually having the kind of incentives to drive the kind of behavior that we're talking about.

Recently the PCI [[Payment Card Industry](#)] compliance mandates actually have specific financial incentives and penalties tied to them. And so they're getting a lot more attention in the industry these days because the ROI of becoming secure versus the penalties and potential loss of opportunity to do business due to the removal of being able to transact commerce through credit cards is significant and it's much more than the cost of actually becoming compliant.

Similarly, the disclosure laws in California are having a broad reaching affect and creating awareness no only across the industry and forcing disclosures about breaches and loss of information and loss of data which is causing all the enterprises to take action.

As Catherine says, people don't want to lose their reputation and be the next person that hits the front page of the newspaper with some sort of negative branding impact.

More importantly, though, it's also creating a broad awareness in the large population. I mean, the marketplace itself.

Individuals who now conduct business are starting to conduct business with those companies that they believe are more secure. We're actually seeing marketing by organizations about their degrees of security, because they're trying to satisfy a population who's now becoming much more aware of the risk of data loss and the personal impact that that could have to them.

So we're starting to see this kind of symbiotic relationship developing between the enterprises and between the individual consumers themselves as a result of the legislative mandates and disclosure laws coming together at the same time.

KNECHT: So will compliance with regulations and government mandates alone help to keep these enterprises secure or keep data losses from happening at the levels that they have in the past? Or do enterprises really need to think beyond that towards processes related to risk management on a broader level?

MANN: Well, I think there are two issues that I think are on the horizon that are going to be difficult to deal with. One is the extent to which security breaches may emanate from outside the legal jurisdiction of our own laws.

Once you have this potential for multiple standards around the world, then you have the opportunity for what we as economists call regulatory arbitrage. You know, wherever the regulations are lightest, that's where you're going to have the hackers sit or the data go.

And so this is not a new problem associated with security issues; it comes up in banking regulation, for example, very clearly. But it's nevertheless something that is, it's not even on the horizon, I'd say it's here right now, in trying to deal with this issue.

EVANS: Right. The challenge we have is that the business model for security is essentially broken. Point product solutions have been delivered to sell point product issues. We had viruses, we came up with antivirus. We had spyware, we came up with anti spyware.

And in so doing, we stacked up numerous boxes within the enterprise space such that the cumulative average or the annual growth rate for spending on the labor to manage the complexity of security is actually growing three times faster than the average growth rate of the IT budget itself. Right, and that that's a business problem.

And most customers are saying we need to move to much more of a horizontal approach to security that cuts across this heterogeneous environment to deliver cost and complexity improvement because while we're adding more technologies and exponentially more cost to the problem, the degree of protection is not following.

And so what we're seeing is kind of this idea of opening up kind of to open APIs and open standards into which any security innovation can plug into in more of a platform approach. And the platform itself like the human immune system becomes almost self monitoring and self remediating where as opposed to kind of the stacked box approach.

Is the industry there yet? Not quite. Is it something that we as the vendors need to take on as an approach to actually deliver a better security economics to the industry itself and assist the enterprises in solving the problem?

Absolutely. And you'll see major vendors going in that direction, and it's part of the reason you're seeing consolidation with the industry so you can build a critical mass around those kinds of solutions.

KNECHT: So, Peter, you mentioned at one point that the industry is not quite there yet in terms of moving to kind of a more holistic approach to security. But with recent major risk issues, particularly in the financial services industry, what do you think it will take to get them, to get the industry to pay attention? Or is there a major issue upcoming that will turn the industry on its head and start to think in a different way about security?

EVANS: Yes, I think we've actually already hit the major issue, because the current spending model cannot continue. And so we're seeing a lot of pressure back on the vendor community and on the industry to create more integrated solutions, to create more consolidated approaches and to start thinking of security as an enabler of business value as opposed to a necessary evil to protect some new innovation within the enterprise itself.

So the industry is already speaking, and it's already telling the vendor community what it's looking for in terms of solutions. It's why you're seeing companies like IBM and some of our major competitors starting to bulk up to deliver those integrated solutions.

KNECHT: If there's one thing that you could tell enterprises to do today to improve their security posture, what would it be?

MANN: Enterprises have to recognize that the potential loss to their brand of losing somebody's data, that that is increasingly large.

And there have been studies on whether or not a company is punished through loss of sales. There are studies that focus on whether a company is punished through loss of stock price.

I think what should be perhaps most on the minds of companies is what is going to happen when lawsuits get involved because those have, you know, the sky's the ceiling, the sky's the limit on what a company might have to pay when you start getting class action lawsuits as the outcome. And a company should not take that possibility lightly.

KNECHT: Peter, same question to you.

EVANS: From a technology perspective, I don't think I have one answer; I have maybe two or three recommendations.

The first is, you know, as we talked about earlier on this podcast data is the new currency. That's where the value resides within the business, not only in terms of how to profit from that data, but it's also the life blood of effective operation of the enterprise itself.

You know all the supply chain solutions, and ERP and CRM and these sorts of things that will expect accuracy of data are irrelevant if the data itself isn't protected. And that's a new set of thinking that the enterprises need to start looking at how they manage data, how they archive it, how they protect it, encrypt it and put the right sets of solutions around that. So there needs to be a new set of thinking.

The second recommendation is to move the mindset from virus protection to [malware](#) protection because malware and all the new forms in malware are actually the vehicle by which profit is generated.

A lot of the viruses are really about disruption. And so that's a shift in thinking from old school security thinking to more about how to think in a way the malicious...the folks who know malicious intent are actually going about cutting profitability.

Everyone is on all sorts of distribution lists and information feeds for the latest viruses and signatures and vulnerabilities and things like that. If anything, get on one list that talks about the new forms of malware and the new forms of attack in a malware world because that is where the profit is being created and that's where the most destruction is being created.

KNECHT: Great. Catherine and Peter, thank you so much for your time.

MANN: A pleasure being here.  
EVANS: Thank you very much.  
KNECHT: And good evening.  
[END OF SEGMENT]

To continue the discussion, visit the [Frequency X blog](#).