SentinelOne
The future of endpoint security

C-Level IT Security Priorities With Jeremiah Grossman

Addressing Cyber Attacks and the Future of the Cyber Insurance Market

Jeremiah Grossman has lived a literal lifetime in computer security. His career spans nearly 20 years during which he has become one of the industry's biggest names, receiving a number of industry awards and public thanks for his security research from major companies such as Microsoft, Mozilla, Google, and Facebook. He has been a guest speaker on six continents at hundreds of events, including many top universities, in addition to authoring hundreds of articles and whitepapers. He is the former information security officer for Yahoo! and the Founder of WhiteHat Security, which today has one of the largest professional hacking armies on the planet.

Jeremiah currently serves as the Chief of Security Strategy for SentinelOne.

Currently, Jeremiah serves as Chief of Security Strategy for cyber security firm SentinelOne

Cybercrime projected to cost the world in excess of $6 trillion annually by 2021 according to Cybersecurity Ventures.

Companies find themselves scrambling to protect themselves and their users' data, and to mitigate financial losses in the face of the next inevitable attack. SentinelOne's Chief of Security Strategy, Jeremiah Grossman, shares his expertise and insights into some of the more pressing security challenges that face C-level executives today.

What are some concerning gaps you see in the solution approach to protecting organizations?

Unfortunately, the best driver for an organization to really get secure is to get hacked. People generally do not put on a pair of running shoes to run a mile until they have a heart attack. If you look at all the breaches, they all have to do with the exploitation of insecure software. What the industry largely buys in response is firewalls and encryption—which are both fine, but both fail to address the fundamental problem. The gap is in our failure to understand what the problem actually is. The real solution is that we need to fundamentally improve the security of the software, but that answer is very complicated for companies. It is much easier to just buy a box with blinking lights that say 'You are secure now' than it would be to invest in the underlying security of the software itself.

There is also a great disconnect between the way the CFO of any major company invests in IT, versus the spending priorities of the CTO, whose number one job at the company is to protect the company's IT assets. If you ask the CFO of any major company how the business invests in IT (not IT security), it's software and software development, followed by hosting, and then the least of the three is on networks and routing equipment. Conversely, the largest pool in the CTO's budget is spent on firewalls to protect the network, then on endpoint protection to protect the hosting, and lastly on software security. If you look closely, you will see that the spending priorities are backwards— meaning that this is a spending priority issue more than anything else. Unfortunately, this kind of inequity of spending is practically baked into law because of regulatory compliance and therefore is very difficult to change.

Why have you personally taken an interest in the cyber insurance market?

I like staying on top of what is going on in the market, and I do so by simply following the money. For example, Infosec today spends roughly 75 billion dollars on their budget every year. This is the amount we spend on products and services, and our market is growing at about 5% annually, which equals about 3.4 billion dollars being added to the budget every year.

Cyber insurance, on the other hand, is only valued at 3 to 4 billion in premiums at the end of 2016. However, the market has been growing over the past 4 years at a rate of about 60-70% annually. If you compare and contrast the new money going into Infosec, versus the premiums being paid on cyber insurance, the money is almost equal. This means that when a company has budget to spend on security, they are now just as likely to spend it on cyber insurance as they are to prevent a security breach. Looking towards the future, I believe that cyber insurance companies will be increasingly telling companies what products they need to buy, and what to implement, and this will filter down to influence the rest of the market.

"When a company has budget to spend on #security, they are now just as likely to spend it on cyber Insurance"

Click to tweet

Is the growing investment in cyber insurance speaking to the fact that companies do not have the faith that they can prevent hacks?

CSOs and CFOs don't really believe that over a given year they will be able to prevent all potential hacks, nor that there's anything they can do to prevent them. And why should they think otherwise? It's not like security vendors will give a warranty for the products or services that they sell. Actually, I am pretty passionate about solving that issue— security vendors must start offering a warranty for their products and services because we are in the midst of a credibility crisis and the beneficiaries of that are the cyber insurers. Additionally, cyber insurance is pretty inexpensive, which is why everyone is buying it in droves. The current cost of a cyber insurance premium is about 1% on average of the covered amount, meaning a million dollar policy will cost a company only 10k annually.

"We are in the midst of a credibility crisis and the beneficiaries of that are the cyber insurers"

Click to tweet 

How is the effectiveness of a cyber security program measured? Is there a measurable ROI?

There is no real ROI in the security business, it's more about loss avoidance than anything else. So how do you measure security? That is clearly the biggest challenge. I like the idea of— are you getting hacked or not? Are your fraud rates going down? Are your account takeovers going down? In other words, is the ratio of the amount you are spending versus the amount you are protecting becoming more favorable? If you have a break-in or a loss, that is ok, but is it within your predefined level of tolerance?

These are some of the questions companies need to be asking themselves when it comes to measuring the effectiveness of their IT security. That being said, most companies do not have good metrics or ratios for this, even though it is something they all should definitely have. Before a company can create the necessary security statistics, they have to first have a very clear understanding of the value of everything that they need to protect.

How do you believe the disconnect between the C-suite and security endangers enterprises?

It is a big challenge to get resources and approval from the decision makers when they do not see eye to eye with the security department. This would create in impossible situation, especially when the business sees you as an impediment to moving quickly. It reminds me of when I was off-road racing in a 7-Series BMW with a V12 engine only to discover moments before the race that the brakes went out...I mean, If you are going to race a powerful car with no brakes, how fast will you go? If I really want to show the risk associated with cyber problems so that they are both relevant and comprehensible to the C-suite, I just show them how to hack. Once they see how easy it is to cause a massive amount of damage, all of a sudden they become interested. They are not completely educated at that point, but you do have their attention. Teaching hacking is probably the best thing we can possibly do to both bridge this disconnect, and to demonstrate vulnerabilities.