# USING INTELLIGENCE DATA IN A NEW ERA OF CYBERCRIME



By PYMNTS (HTTP://WWW.PYMNTS.COM/AUTHOR/PYMNTS/)

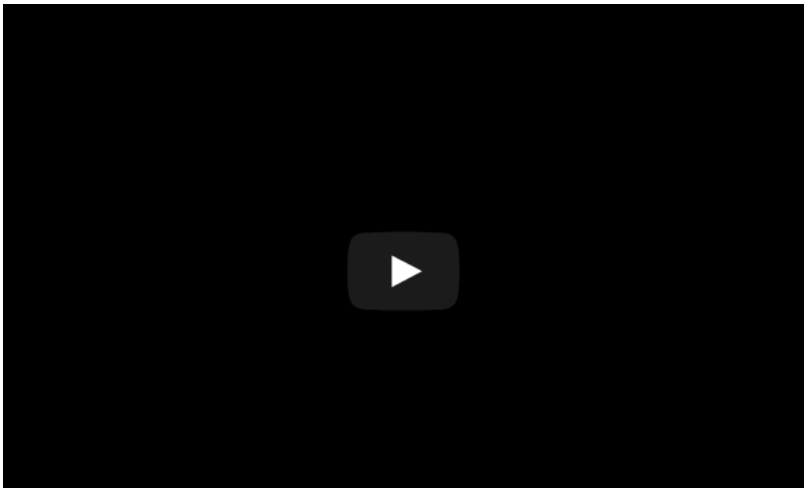
@pymnts (http://twitter.com/@pymnts)

What's Next In Payments®

31

6:15 AM EDT April 14th, 2015

They're smart, they're well educated, they're organized, and they're well funded. They're nimble and resourceful – when one door closes, they find new ways to get things done. Those are just a few of the frightening attributes of the new era of cybercriminals, noted **MPD CEO Karen Webster** in a recent digital discussion with **ThreatMetrix Director of Product Marketing, Ken Jochims.** So what's the secret to stopping these highly motivated bad guys before it's too late? Get Jochims' expert insight on the scale of cybercrime today, how global crime rings operate and the best ways to conquer the "financial cyber kill chain."



## WHAT'S HOT

MERCHANT INNOVATION
NCR Platform Takes ATM Ecosy The Cloud
(http://www.pymnts.com/news/2015/n platform-takes-atm-ecosystem-to-the-cl

INTERNATIONAL
Alibaba Health Absorbs Tmall's Pharmacy in $2.5B Deal
(http://www.pymnts.com/news/2015/a health-absorbs-tmalls-e-pharmacy-in-2-5

MOBILE COMMERCE
Uber Drives Deals for Samsung S6 Owners
(http://www.pymnts.com/news/2015/u drives-deals-for-samsung-galaxy-s6-own

NEWS
Measuring The Speed Of Theft
(http://www.pymnts.com/news/2015/n the-speed-of-theft/)

VIEW ALL AR

(/tag/whats-hot)



## YOU MAY ALSO LIKE

MERCHANT INNOVATION
NCR Platform Takes ATM Ecosy The Cloud
(http://www.pymnts.com/news/2015/n platform-takes-atm-ecosystem-to-the-cl

INTERNATIONAL
Alibaba Health Absorbs Tmall's Pharmacy in $2.5B Deal
(http://www.pymnts.com/news/2015/a health-absorbs-tmalls-e-pharmacy-in-2-5

NEWS

## THE SCALE OF CYBERCRIME

After MPD CEO Karen Webster began the discussion with a profile of today's intelligent, conniving cybercriminal, ThreatMetrix's Ken Jochims jumped in to talk the scale of cybercrime. And when we look at the global numbers, he said, the reality is staggering. About 378 million people are victims of cybercrime each year, translating to over 1 million victims daily – or 12 victims every second.

The fallout, said Jochims, is clear – it's economic loss that is primarily aimed at banking and eCommerce customers, since the easiest way to attack a business is indirectly through its customers.

So who is behind these crimes?

## INSIDE GLOBAL CRIME RINGS

"To understand who's behind all of these threats, you have to realize we're up against a global criminal presence that in many cases is decentralized in that they are loosely connected, working almost like flash mob cybergangs coming together for targeted operations," said Jochims.

More traditional gangs like the Russian ones have amassed the largest known collection of stolen Internet credentials, including 1.2 billion username and password combinations and more than 500 million email addresses. These organizations have even created business models that could best be described as the CyberCrime Industrial Complex, explained Jochims, with vendors providing any number of tools and services featuring custom malware, support contracts, bulk distribution of personal info or stolen credit card data with replacement guarantees of failed cards, and more.

"Their collective efforts seem to be escalating hoping to cash in by utilizing all the reconnaissance and data gathering from the massive data breaches from last year," said Jochims.

**That prompted Webster to ask, why is it so much worse? Is it because the business has become much more organized, and there are more tools available?**

"A big part of it is the profit – these guys are making a lot of money doing this. The chances of being caught are extremely low if they're reasonably smart about how they do the crime. If you're in Russia and you're a cybercriminal, the only thing you don't want to do is attack a Russian bank or business. Other than that, everyone else is fair game," he said.

Cybercriminals will also use different servers to hop across multiple countries, and when they do that, policing capabilities disappear. They cross multiple jurisdictions, and in many instances we don't even know where they're coming from.

## COMPLEX FRAUD CHALLENGES

All attacks start with a multitude of technologies, techniques and skills ranging from malware, social engineering, and various forms of phishing, all with the goal of obtaining credentials to compromise accounts, said Jochims.

Then there's malware, which Jochims said has taken a backseat lately with the focus on data breaches. But with a staggering daily growth rate that is more than doubling year over year, it won't be long before it makes a comeback.

**Webster then asked, "So when we think about payments and the threat to the ecosystem, how are they getting access to data and credentials to be breached?"**

Generally, attacks are happening through some kind of phishing expedition, said Jochims. Target was the classic example where a contractor who was not an employee but was allowed access into the system happened to be the target of a phishing email scam.

**"We've all heard the statistic about how these guys are rooting around systems for hundreds of days without being observed. Why?" asked Webster.**

"Well, what they're doing is using stolen credentials. If they're using an administrator's stolen credentials, they're not setting off any flags inside the company. They'll come in and enter an ID and password and then they're allowed access. Nothing is blocking them," said Jochims. "Ultimately, one of the ways we help stop that is that we can identify where someone is coming in from."

No Credit Card? No Problem, S Millennials
(http://www.pymnts.com/news/2015/n card-no-problem-say-millennials/)

MOBILE COMMERCE
Uber Drives Deals for Samsung S6 Owners
(http://www.pymnts.com/news/2015/u drives-deals-for-samsung-galaxy-s6-own

VIEW ALL AR
(/category/mobile-commerce)


(http://www.pymnts.com/apple-pay-ec tracker/)

## GROWING MOBILE FRAUD

With the growth of the mobile channel comes a direct onslaught of large scale attacks – mobile malware is up over 700 percent with millions of new strains being discovered daily, and that's only the ones being found, said Jochims.

"Today's malware is especially good and not being discovered due to its ability of malware to change functionality, embed itself at the core of a computer's operating system and be so easily distributed through SMS downloads or fake app stores."

**Webster added that we saw that with Apple Pay – the payment process is secure, but the provisioning of accounts using stolen credentials enabled the bad guys to buy merchandise from Apple using bad credentials.**

And, all of this is being made worse by the fact that mobile devices are coveted possessions for the owner as well as the criminal, said Jochims.

"The mobile device knows where you've been, who you know, what networks you use, where you shop and bank – everything that makes it exceptionally valuable to the bad guys whether they take physical or virtual possession of it."

Mobile users are also pretty careless with how they use their devices, not understanding what mobile-based phishing attacks may look like, and with their willingness to download and try all kinds of apps. The potential payoff for criminals is high.

## THE GLOBAL COST OF PAYMENT FRAUD

As is clear from the Nilson report results depicted in the webinar, card not present fraud is gaining more momentum and it's a trend that shows no signs of stopping, said Jochims. With the shift to EMV in the U.S., Jochims said two fraud spikes are expected to occur later this year – the first as criminals use up their supply of magstripe-based stolen card data, and then again as they shift to the online space.

**"So the bad guys will get better, and we wont keep up. Is that how you interpret the statistics?" asked Webster.**

Jochims said that it was, because they're efficient and they only have to be right once. They will try multiple ways to attack.

"There's a real need for information sharing among our customers – but if they don't provide that, it's not broad enough to look globally to understand threats and risks out there."

**Webster then asked, "Why is the rate of fraud in general going to increase? Haven't we become smarter?"**

"You'd hope so," said Jochims. "But if a solution is implemented that's a few years old, it may have stopped early attacks, but bad guys are getting smarter with the way they attack. They're moving around traditional barriers to fraud. We've seen businesses not spend a lot on a solution, just not get that box checked – they aren't seeing it as a large enough problem."

**"Is it also because there is so much friction built in already to transacting on a mobile device that merchants are interested in conversions?" asked Webster.**

Jochims said that was a reasonable take, but another part of the problem is that credit cards are increasingly being stored on merchant websites for easier checkout. That stored information represents an easy target for criminals to turn stolen credentials into cash. In addition, from their eCommerce customers, ThreatMetrix has seen an expansion of fraud attacks from traditional card-not-present (CNP) attacks to newer account takeover attacks.

## THE RIGHT FRAUD PREVENTION SOLUTION

According to ThreatMetrix, many fraud prevention solutions assume guilt before innocence, resulting in top line loss due to transaction abandonment and creating a problem far more costly to businesses than fraud losses.

Shopping cart abandonment rates are one of the causalities resulting from complex anti-fraud solutions. For eCommerce, more than 68 percent of shopping cart visits are abandoned. Of those abandoned, more than 30 percent of customers blamed excessive security checks, lack of confidence in site security and declined authorizations as the reason.

security and declined authorizations as the reason.

The solution to stopping cybercriminals, not customers, is to quickly understand the difference between trusted users and cybercriminals, in real time, said Jochims. ThreatMetrix's approach to this kind of analysis includes:

- Analyzing billions of transactions
- Across hundreds of millions user accounts
- From thousands of websites and mobile applications
- To provide frictionless customer access, stopping fraud to protect brands and their customers

**"We talk about the payments 'Uber experience' that doesn't involve any interaction between the consumer and the business. How does that experience impact what you're describing in terms of protecting the consumer as well as merchant/bank against fraud?" asked Webster.**

For the users gaining access, transparency is key, said Jochims. People want security, but don't want to have to work to get it. There needs to be a concept of transparency. ThreatMetrix approaches it in three phases – device analytics, identity analytics and behavior analytics.

After explaining how each of these phases work, Webster asked Jochims what about ThreatMetrix's portfolio of solutions made it different from others in the market.

The biggest competitive advantage, he said, was the shared network. ThreatMetrix has 3,500 customers throughout the world, and all of the information about their users is anonymized so that everyone can share and use that information.

So is it working? From a survey ThreatMetrix ran last summer though TechValidate, these customers and others told ThreatMetrix that over 70 percent of respondents saw a 20+ percent reduction in fraud rates with almost 20 percent of respondents seeing reductions of over 60 percent.

"One of the major benefits [of] stopping fraud at the front door is the follow-on benefit of reducing chargebacks, and from what customers tell us we're helping their bottom line by reducing charge backs more than 20 percent for over 60 percent of our customers," Jochims explained.

**Webster asked, "How do you advise your merchants on what an acceptable level of fraud is, and does that vary per merchant category or time of year?"**

"I think it depends a lot on what the risk threshold of a particular business is. Banks certainly have a different threshold for commercial customers than they do for retail customers. Depending on the type of eCommerce business it is, it will have its own level of acceptable risk," said Jochims.

Over time, he added, that might change, as bad guys get more sophisticated. It also might change seasonally. During Christmas, for example, some merchants dial back on fraud methods to increase business. They do their own math to determine if that's worth it.

"It always comes down to an economic decision. It's a business-level discussion."

**As the conversation came to a close, Webster asked, "We talk about prevention vs. detection. I know they're two sides of the same coin, but what's the goal in thinking of strategies to mitigate the risk of cybercrime? Is it preventing access, or detecting they're a threat?"**

"The general industry approach is about layered security – you'll hear that term used a lot," said Jochims. "But trying to stop as many bad guys at the front door as possible is key – that's our goal."

Topics: Featured (http://www.pymnts.com/tag/featured/)

What's happening now (http://www.pymnts.com/tag/whats-happening-now/)

## COMMENTS

## ALSO BY THIS AUTHOR

*1723 New Articles This Month*

MERCHANT INNOVATION (http://www.pymnts.com/category/news/merchant-innovation/)

NCR Platform Takes ATM Ecosystem To The Cloud (http://www.pymnts.com/news/2015/ncr-platform-takes-atm-ecosystem-to-the-cloud/)

INTERNATIONAL (http://www.pymnts.com/category/news/international/)

Alibaba Health Absorbs Tmall's E-Pharmacy in $2.5B Deal (http://www.pymnts.com/news/2015/alibaba-health-absorbs-tmalls-e-pharmacy-in-2-5b-deal/)