2019 CURRENT STATE OF CYBERCRIME
The Digital Transformation of Cybercrime
EXECUTIVE SUMMARY

Organizations across industry and government are exploring exciting new opportunities through the digital transformation of their operations—adopting digital technologies like mobile, cloud and IoT to operate more efficiently, collaborate more effectively and create new channels through which to deliver innovation in the marketplace.

But guess what? So are cybercriminals.

That’s right: Digital transformation is making it easier not only for legitimate organizations to expand their reach but also for fraudsters and other bad actors to expand theirs. For example, cybercriminals are increasingly using mobile to ply their trade, as evidenced by a 680 percent increase in fraud transactions from mobile apps between 2015 and 2018.

RSA expects to continue to see digital transformation unfold for both legitimate businesses and the cybercriminals who target them for fraud. This report explores this digital revolution that both sides are experiencing and examines its implications for fraud and other forms of cybercrime in 2019.

We will look at the digital developments, market forces and regulatory pressures that are driving this shift in how fraudsters and others commit their crimes, as well as how anti-fraud forces fight them. Based on insights gleaned from RSA research and other sources, we will focus on three key trends:

1. Growing use of mobile to commit cybercrime
2. Adoption of legitimate digital platforms for illicit activities
3. Use of advanced technologies both to commit and to fight cybercrime

680% increase in fraud transactions from mobile apps (2015-2018)

Source: RSA Anti-Fraud Command Center data, October 2015-December 2018
Fraud in the mobile channel has grown significantly over the last several years, with 70 percent of fraud transactions originating in the mobile channel in 2018. In particular, fraud from mobile apps has increased 680 percent since 2015. In another indication of the growing popularity of mobile as a channel for cybercrime, the use of rogue mobile applications to defraud consumers is on the rise. RSA identified an average of 82 rogue mobile applications per day last year across most popular app stores.

We expect the popularity of the mobile channel for fraud will continue through 2019, especially as cybercriminals keep finding ways to introduce tactics and technologies such as phishing and malware to the mobile channel. For example:

- **Smishing** uses SMS texts rather than email to deliver phishing messages aimed at getting victims’ account credentials, credit card numbers, etc.
- Mobile 2FA phishing is a variant of smishing in which the account takeover attempt is specifically designed to bypass two-factor authentication.
- Mobile malware works like traditional malware to attack and disable a user’s device, but specifically targets mobile devices, with developers constantly enhancing the malware to keep up with new versions and security patches of mobile operating systems.

The RSA Anti-Fraud Command Center expects these and other forms of mobile-based cybercrime to evolve and grow even more prevalent as organizations continue to leverage the mobile channel to deliver new digital services to customers.
Watch for: Cross-Channel Vulnerabilities

While fraud growth in the mobile channel continues to trend upward, it is by no means the only digital channel that fraudsters are exploiting. As organizations continue to introduce innovative products and services online, in the cloud and across other digital channels, cybercriminals can be expected to seize on these developments to launch more attacks. In this scenario, we see that the very advances that fuel innovation and growth of digital channels also fuel cross-channel fraud. This is one of the ways in which digital transformation creates both digital opportunity and digital risk.

Consider the move to an open API economy, in which organizations can more easily share data (and in some cases may even be required to do so by regulations such as the EU’s Payment Services Directive II, or PSD2) in the interest of customer convenience. This results in innovations such as consumers being able to share account information with apps and platforms of their choice. For example, a consumer can choose to securely share financial data with an app that provides financial planning. But it also creates a vulnerability across channels that cybercriminals will be eager to exploit.

Or think about how an increase in cybercrime can accompany the introduction of a new digital service. For example, the RSA Anti-Fraud Command Center saw phishing attacks increase 178 percent after leading banks in Spain launched instant transfer services. Cybercriminals are always alert to these types of developments and quick to seize on them for their own nefarious purposes.

THE TAKEAWAY: As one analyst put it last year, “A range of channels means a range of targets for criminals.” The analyst’s report, sponsored by RSA, points to the importance of an omnichannel fraud management strategy, with recommendations to leverage data from across channels to identify risk and remediate identified vulnerabilities across channels. The report also cautions about the tendency of organizations to use a different point solution for every channel in the attempt to fight omnichannel fraud, an approach that is inefficient—and also ineffective, because most often these tools are not configured for cross-channel awareness of fraud activity.

Still Phishing After All These Years

Mobile may be taking center stage as an increasingly popular vehicle for cybercrime, but that doesn’t mean the end of tried-and-true methods like phishing. To the contrary, phishing increased 12 percent and accounted for 47 percent of all fraud attack types RSA detected in 2018. It still works, and it’s not likely going away anytime soon.

Source: RSA Anti-Fraud Command Center

57% of companies use up to 10 different anti-fraud tools to manage fraud across channels

USING LEGITIMATE PLATFORMS FOR ILLICIT ACTIVITY

Social Media: The New Public Square for Fraud

In the 2018 Current State of Cybercrime, RSA reported on a fast-growing trend of cybercriminals relying on Facebook, Instagram, WhatsApp and other legitimate social media and messaging platforms to communicate with each other and sell stolen identities, credit card numbers and other ill-gotten gains. Our prediction that this trend would expand and continue has been borne out. By the end of last year, social media fraud attacks had increased 43 percent, as cybercriminals continued to find new ways to exploit social media platforms for gain.

One such development involves the Telegram bot feature that is being used by cybercriminals to facilitate and automate their activities. Some provide automated tools for common actions to enhance communications, whereas others provide actual fraud services via online stores. RSA Anti-Fraud Command Center findings suggest trading in stolen identities will gain even greater momentum, with more stores likely opening on legitimate platforms to sell this type of data. Given the ease of use, absence of fees and other benefits of these platforms, continuation of this trend in 2019 should come as no surprise.

43% increase in social media fraud attacks in 2018

Source: RSA Anti-Fraud Command Center
Using Mobile to Stay Low-Profile

RSA is seeing cybercriminals use mobile not just as a vehicle for launching phishing, malware and other attacks but also as a platform for resources that make it easier for them to carry out criminal activity and get away with it. In addition to using legitimate mobile apps for nefarious purposes, they are also developing their own apps to increase their anonymity, avoid detection and otherwise keep anti-fraud forces from tracking them down and exposing what they’re doing, as RSA has reported.³ We can reasonably anticipate that this activity will continue to grow as cybercriminals become increasingly emboldened by their successes.

The Advantages of Blockchain for Cybercriminals

RSA reported last year² on the use of a blockchain-based domain name system (DNS) to host sites such as stores that sell credit card information or other stolen data. Unlike traditional DNS addresses, which are subject to oversight by governing organizations like ICANN, blockchain-based DNS addresses have no oversight. That makes it harder for law enforcement to interfere with their operations, including taking down sites, and that makes the popularity of blockchain among cybercriminals likely to grow. This is one reason RSA anti-fraud experts are predicting more fraud websites will be utilizing blockchain domains in 2019.

Cybercriminals are developing their own apps to increase their anonymity, avoid detection and otherwise keep anti-fraud forces from tracking them down and exposing what they’re doing.
Watch for: Exploiting On-Demand Services Platforms

What’s the next frontier for cybercriminals looking for legitimate online platforms they can exploit? CNBC recently reported on the use of on-demand services platforms such as Uber and Airbnb to launder money made from credit card fraud: “Money laundering is an essential element in the proliferation of cybercrime, as much of the funds come in the form of cryptocurrencies with a chain traceable to crime.”

Using on-demand platforms to hide ill-gotten gains is one thing; using them to actually commit fraud is another. But it happens: CNET has reported on Uber drivers being victimized by fraudsters, who impersonate the company’s driver support team to cancel a ride, get the driver’s Uber account credentials and then use them to steal the wages in the account before they are transferred to the driver’s bank.

THE TAKEAWAY: On-demand services platforms have not yet reached the level of exploitation by cybercriminals that other legitimate digital platforms have seen. The hope for keeping it that way lies in on-demand businesses taking all precautions possible. Perhaps the most important is instituting digital risk protection capabilities, which enable organizations to:

- Closely monitor their externally accessible domains and apps
- Collect and analyze digital risk-related data from the dark web
- Quickly and effectively respond to digital risk events

In addition to implementing robust anti-fraud solutions that monitor for digital risk, RSA encourages adoption of the 3D Secure 2.0 protocol, which promotes the use of risk-based authentication to detect fraud in card-not-present transactions.

“Money laundering is an essential element in the proliferation of cybercrime, as much of the funds come in the form of cryptocurrencies with a chain traceable to crime.”
FIGHT FIRE WITH FIRE: DIGITAL CRIME AND CRIMEFIGHTING

The trend toward using the latest digital technologies in cybercrime increasingly applies both to committing and fighting cybercrime. Here are some examples of how both sides are making the most of advanced digital capabilities. Watch for 2019 to bring more cybercrime that’s based in automation and IoT—as well as more anti-fraud capabilities that are technology-driven.

52% of financial institutions are planning to adopt an authentication hub in the next 1-2 years

Source: Aite Group, Current and Future FI Fraud Loss Trends

<table>
<thead>
<tr>
<th>CYBERCRIMINALS</th>
<th>CYBERCRIME FIGHTERS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fraud Automation</strong></td>
<td><strong>Self-Learning Risk Engines</strong></td>
</tr>
<tr>
<td>Just as in legitimate business activities, automation makes it possible to do a lot, a lot more quickly. Want to verify thousands of stolen usernames and passwords in minutes? Use an automated account-checking tool like Sentry MBA or SNIPR.</td>
<td>Today’s risk engine technology uses sophisticated machine-learning models to automatically adapt its assessments of fraud risk, based on what it learns over time. The RSA Risk Engine is just one example.</td>
</tr>
<tr>
<td><strong>IoT</strong></td>
<td><strong>Behavior Analytics</strong></td>
</tr>
<tr>
<td>The more IoT devices become part of everyday life, the more cybercriminals are going to find ways to exploit them. So how can you trust your self-driving car to get an oil change without taking you for a ride financially? Being able to spot risky behavior in human-not-present transactions is critical to preventing fraud.⁶</td>
<td>Fighting cybercrime is about identifying the good guys as well as the bad guys. That increasingly means using behavior analytics to detect whether people and things are interacting with someone’s accounts and information in expected ways—and being prepared to act quickly when they’re not.</td>
</tr>
<tr>
<td><strong>Cross-Channel Fraud</strong></td>
<td><strong>Authentication Hub</strong></td>
</tr>
<tr>
<td>Cybercriminals are exploiting the growth of cross-channel vulnerabilities by using one channel to break into another. One of the most common examples is a type of account takeover in which a fraudster interacts with an organization’s call center to change the password in order to gain access to an online account. Aside from web and mobile, 38 percent of organizations cite the call center as the channel they’re most concerned about for fraud vulnerability.⁷</td>
<td>One of the most effective weapons for fighting cross-channel fraud is an authentication hub, which provides a central point of visibility from which to detect fraud across channels. Given the growing concern about cross-channel fraud, it should come as no surprise that more organizations are adopting this technology. In the financial services industry, for example, 52 percent of financial institutions indicated they would be adopting an authentication hub in the next one to two years.⁸</td>
</tr>
</tbody>
</table>
CONCLUSION

As organizations become increasingly digital, the challenge of finding and fighting cybercrime becomes tougher. In a relatively short time, we’ve gone from individuals presenting themselves in person when making purchases to not being present at all, across a multitude of transaction channels—even to the point of being represented by devices in the age of IoT. Cybercriminals are exploiting this trend, both by taking advantage of the increasing difficulty of authenticating identities and by taking advantage of digital technologies themselves. As the digital transformation of both business and cybercrime continues, organizations must be increasingly vigilant, and increasingly well-equipped technologically, to protect themselves from sophisticated attacks. In this way, digital transformation becomes both a critical contributing factor in the problem of growing cyber risks today—and a critical resource for solving it.

1 Javelin Research, Overcoming the Top Ten Challenges to Omnichannel Fraud Management, November 2018
2 RSA, 2018 Current State of Cybercrime, July 2018
3 RSA blog, “Five Mobile Apps in Every Cybercriminal’s Toolbox,” October 4, 2017
4 CNBC, “How criminals use Uber and Airbnb to launder money stolen from your credit card,” February 7, 2019
5 CNET, “Con artists are fleecing Uber drivers,” June 28, 2018
6 RSA blog, “Transaction Protection in a Human-Not-Present Age,” June 6, 2017
7 FS-ISAC Poll, “Top Ten Omnichannel Fraud Management Challenges,” November 27, 2018
8 Aite Group, Current and Future FI Fraud Loss Trends, January 29, 2019
ABOUT THE RSA FRAUD & RISK INTELLIGENCE SUITE

The RSA Fraud & Risk Intelligence Suite helps organizations manage fraud and digital risk across multichannel environments without impacting customers or transactions. The suite offers risk-based authentication and behavior analytics solutions for web, mobile and e-commerce as well as fraud intelligence services to allow organizations to protect their customers across the entire digital journey. The Fraud & Risk Intelligence Suite is deployed at over 5,000 global organizations and protects over 1.5 billion consumers.

ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. For more information, visit rsa.com.