Cybersecurity Is Not About Technology: **It's about the Business of Cyber Crime. Everywhere.**

Traditional security methods are proving futile against today's highly organized gangs of cyber criminals. Needed: a security solution with centralized controls that responds swiftly to real-time threat data — so that your data is protected wherever your people are.

INSIDE

SECURITY

Executive Overview

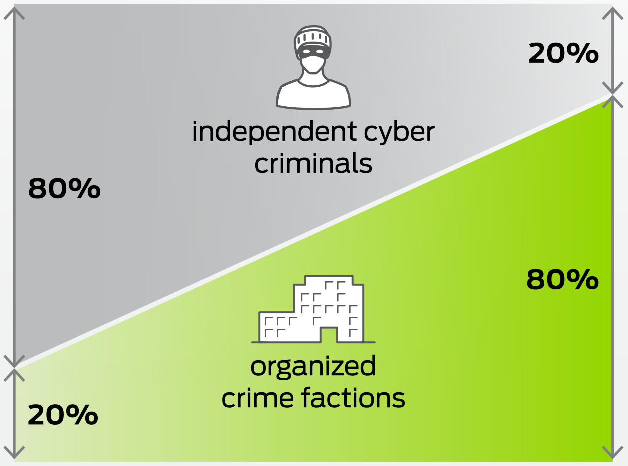
Once the domain of individual freelance criminals, organized crime gangs now control the cyber crime market. A decade ago, approximately 80% of black-market cyber criminals were independent loners with the remaining 20% consisting of organized crime factions.[1] That statistic has been turned upside down. These highly organized gangs of experienced fraudsters operate in the same manner as traditional organized crime families and are proving to be even more elusive to prosecution. Their attacks are highly sophisticated, constantly evolving, increasingly evasive, and carefully orchestrated by experienced fraudsters who have access to infinite resources.

Simultaneously, rapid innovation is driving businesses of all sizes to deploy digitized, cloud-based networks that integrate with the Internet of Things (IoT) in BYOD environments. Although boosting business efficiency and effectiveness, these technical advancements also open many vulnerable back doors to cyber exploits.

In short, the cyber crime market and business environment have both changed radically in recent years. Traditional security methods are proving futile. In this climate, it is imperative that the strategies and technology used to safeguard company networks, data—and overall reputation and brand—keep pace to ensure timely detection and remediation of attacks.

Although no company can protect itself 100% from cyber exploits, we provide a **checklist** of key security best practices that significantly reduce your risk of becoming the next victim.

Cyber crime over the last decade:[1]



Characteristics of organized crime attacks:

- highly sophisticated
- constantly evolving
- increasingly evasive
- carefully orchestrated
- experienced fraudsters
- access to infinite resources

Your Cybersecurity Checklists

Recognizing who your true adversaries are will help you formulate a new strategy for securing your networks and data—in short, your business. You need to change both your perspective and your security strategy going forward.

For starters, start thinking like a cyber criminal. Get into the mindset of an organized fraudster. And come up with a holistic cyber defense that is fast, intelligent, automated, and adaptive.

On the following pages, we present four checklists to follow to make sure your security defenses meet all these criteria.

Intelligent: Do we have the intelligence we need built into our network security measures?

Adaptive: Can we be as agile as the malicious attacks launched by organized crime?

Fast: Do we have the speed we need to stay ahead of organized crime gangs?

Automated: Have we completed necessary essential automation?

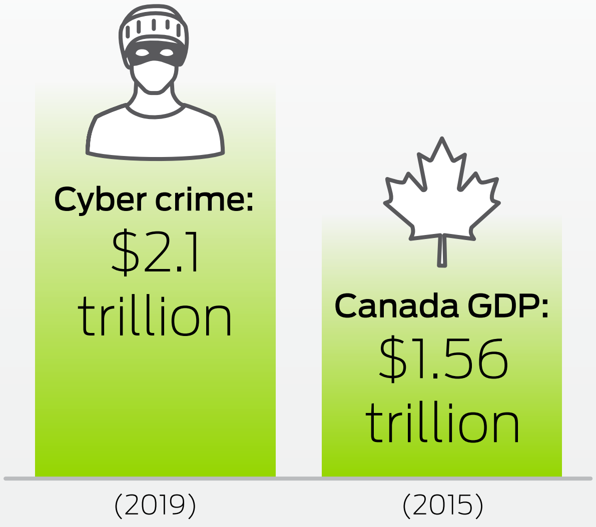
Cyber Crime Is On the Rise

Organized criminals have elevated cyber crime into a flourishing underground economy where the barrier for entry is low and the payouts are large. These highly orchestrated gangs of experienced fraudsters operate in the same manner as traditional organized crime networks—and are proving to be even more elusive to prosecution by law enforcement. Everything from money laundering, to untraceable payment methods, to spoofed domains are weapons in their formidable arsenals. They use “straw” businesses to launder their takings, which are often paid in untraceable bitcoins to secret overseas accounts.

Professional cyber crime gangs have even created “call centers” to support their fraudulent activities.

As businesses rush to cut costs and streamline processes with advanced technologies such as cloud-based networks or the Internet of Things (IoT), they create new pathways for organized crime to penetrate their environments.

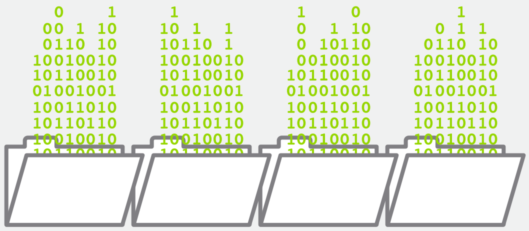
Security experts warn businesses that we now live in a continuous state of compromise. It isn’t a question of if you will be hit by cyber crime, but when.



Cyber crime is expected to become **a $2.1 trillion problem** by 2019. This represents more than the gross domestic product (GDP) of Canada (for the last year that data was available).[2]

2016:

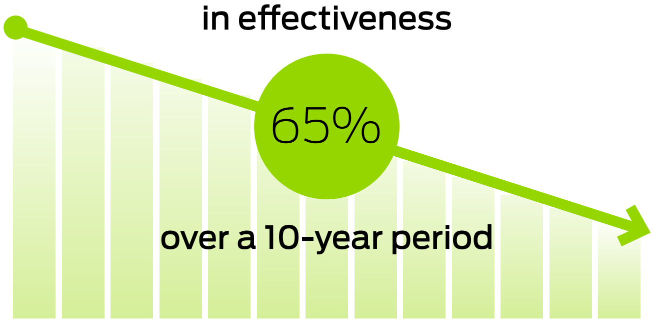
4 billion+ records stolen



In 2016 alone, more than **4 billion records** were **stolen** by cyber criminals.[3]

Intelligent

The second criteria is intelligence—not just human but digital. Security professionals must place themselves in the mindset of organized criminals and invest in intelligent security tools that proactively resist criminal counter-measures.


Sandboxing and anti-phishing security measures diminish in effectiveness

A Juniper-sponsored study by the Rand Corp. found that cyber criminals succeed at countermanding traditional security tactics such as sandboxing and anti-phishing frameworks.[4]

Do we have the intelligence we need built into our network security measures?

□ Our firewall policy enforcement is automated.

□ We have deployed multifactor authentication.

□ We use automated patch management and monitoring.

□ We have isolated our sub-networks.

□ We have adequate network access control.

□ Our integrated security solution can detect threats inside the network as well as at end points.

□ We feed real-time threat data into our network policy engines.

Adaptive

In 2017 we expect to see not only a record number of attacks but also record-breaking losses—including DDoS attacks that result in a 1-terabit data breach.[5] Experts suggest that a key factor driving this explosion in number and size of attacks is the growing base of IoT devices. Organized crime is capitalizing on these new ports of entry by investing in evolving attack scenarios, advanced persistent threat tactics, and dynamic malware exploits. Security technology must prove as agile and adaptive as the malicious attacks launched by organized crime.

Can we adapt?

- □ Our security solution is as agile and adaptive as the malicious attacks being launched by organized crime.
- □ Our security solution has policy engines that are fueled by real-time threat data.
- □ Our security solution has flexible and customizable controls that allow us to respond swiftly to new threat variants.

The Race Is On

By reaching into their deep pockets—which contain virtually unlimited resources—organized crime gangs can invest in the latest innovations and hire some of the world's brightest computer minds to develop cyber threats of ever-increasing sophistication and scale.

Additionally, just like legitimate Internet businesses, organized cyber criminal gangs are creating new revenue streams by offering cyber crime services for hire. Ransomware-as-a-service, fraud-as-a-service, and extortion-as-a-service are now commonplace offerings on the "dark web." By commercializing malware kits and offering as-a-service packages, criminals have also lowered the barrier for entry into this lucrative market for others.

Legitimate businesses simply can't keep up.

Cyber crime was **second highest** reported economic crime

32% of businesses have **already** been infiltrated by cyber criminals

18% are **unsure** of whether they have been compromised

50% of compromised businesses lost more than **$5 million**.

One-third of those lost more than **$10 million**.

Cyber crime is big business throughout the world[6]

Double the ransomware attacks

2017:

10 million DDoS attacks anticipated

Legitimate organizations can't keep up with organized cyber criminals[7]

Fast

With their unlimited financial and human resources, organized crime gangs move at the speed of light. Their attack mechanisms and countertactics elude detection traditional security measures. These attacks are being launched both outside and inside the network.

Do we have the speed we need to stay ahead of them?

- □ We have a rapid-response solution in place to immediately act upon any perceived threat—whether from within or outside the network.
- □ Our centralized control system is capable of speeding deployment of patch management and streamlining policy enforcement across the network.
- □ We have protections woven into the fabric of the network—and not only at the end points—enabling fastest response rate to a detected attack regardless its location on the network.

Traditional Cybersecurity Doesn't Work Anymore

Security professionals are struggling to keep up with cyber criminals. The state-of-the-art environments they are deploying—and charged with protecting—are designed to streamline business processes and accelerate revenues. But they also leave their organizations exposed to dangerous cyber adversaries.

The impact has been devastating. Although companies continue to invest in cybersecurity, they don't have the same resources. According to Gartner, spending on cybersecurity increased 7.9% in 2016, topping $81 billion, as organizations scrambled to stay ahead of cyber criminals.[8]

Yet 2016 turned out to be a record year for cyber crime. We saw the largest data breaches to date, an explosion of DDoS attacks, and an off-the-charts number of ransomware variants. Legitimate businesses simply can't keep up with the criminals.

Traditional security methods simply no longer apply. Companies need a unified network security platform to get the upper hand.

Organizations leave themselves

vulnerable to cyber criminals

as they adopt emerging technologies such as cloud, artificial intelligence, and the Internet of Things without taking appropriate safeguards.

Automated

Although organized criminals have the leisure that comes with deep financial backing, legitimate businesses possess only limited budgets and are forced to do more with less. This makes automation essential.

Automated security updates have proven less prone to counter-measures by organized criminals. Such updates also increase operational efficiency.

Have we completed necessary essential automation?

□ We have invested in automated solutions.

□ We have improved operational efficiency.

□ We can do more with less personnel.

□ We orchestrate streamlined delivery of enterprise applications with customized security.

□ Our automated responses to attacks speed up our ability to detect and respond to cyber exploits.

Stop Cyber Crime with Juniper Networks

The cyber crime market and business environment has dramatically changed in recent years. So must the strategies and technology used to safeguard company networks, data, and brand reputation.

Juniper's innovative security approach detects and remediates threats faster, safeguarding your business from today's cyber crime. Protect your virtual and physical environment with end-to-end, automated and intelligent defense using Juniper's Software-Defined Secure Network (SDSN).

To achieve cybersecurity that truly defeats cyber crime, go to **Juniper Networks' security solutions page**.

Quick Reference: Your Cybersecurity Checklists

Intelligent

Do we have the intelligence we need built into our network security measures?

- □ Our firewall policy enforcement is automated.
- □ We have deployed multifactor authentication.
- □ We use automated patch management and monitoring.
- □ We have isolated our sub-networks.
- □ We have adequate network access control.
- □ Our integrated security solution can detect threats inside the network as well as at end points.
- □ We feed real-time threat data into our network policy engines.

Adaptive

Can we be as agile as the malicious attacks launched by organized crime?

- □ Our security solution is as agile and adaptive as the malicious attacks being launched by organized crime.
- □ Our security solution has policy engines that are fueled by real-time threat data.
- □ Our security solution has flexible and customizable controls that allow us to respond swiftly to new threat variants.

Fast

Do we have the speed we need to stay ahead of organized crime gangs?

- □ We have a rapid-response solution in place to immediately act upon any perceived threat—whether from within or outside the network.
- □ Our centralized control system is capable of speeding deployment of patch management and streamlining policy enforcement across the network.
- □ We have protections woven into the fabric of the network—and not only at the end points—enabling fastest response rate to a detected attack regardless its location on the network.

Automated

Have we completed necessary essential automation?

- □ We have invested in automated solutions.
- □ We have improved operational efficiency.
- □ We can do more with less personnel.
- □ We orchestrate streamlined delivery of enterprise applications with customized security.
- □ Our automated responses to attacks speed up our ability to detect and respond to cyber exploits.

You aspire to cloud-like functionality. Juniper helps you get there by simplifying your journey. A secure environment where you can build without limits. It's cloud excellence for all organizations.

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks that provide agility, performance and value. Additional information can be found at **Juniper Networks** or connect with Juniper on **Twitter** and **Facebook**.

For more information, go to www.juniper.net/security.

Citations:

[1] Markets for Cybercrime Tools and Stolen Information: Hackers' Bazaar. Rand Corporation. 2014. Sponsored by Juniper Networks. http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.sum.pdf.

[2] International Monetary Fund, World Economic Outlook 2016. https://www.imf.org/external/pubs/ft/weo/2016/02/pdf/text.pdf.

[3] IBM XForce 2017 Index. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03140USEN&.

[4] PwC Economic Crime Survey 2016. https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf.

[5] Deloitte Global Predictions 2017. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-deloitte-2017-tmt-predictions.pdf.

[6] Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016. August 2016. http://www.gartner.com/newsroom/id/3404817.

[7] Markets for Cybercrime Tools and Stolen Information: Hackers' Bazaar. Rand Corporation. 2014. Sponsored by Juniper Networks. http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.sum.pdf.

[8] Deloitte Global Predictions 2017. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-deloitte-2017-tmt-predictions.pdf.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701