THE ECONOMICS OF DEFENSE

Modeling Security Investments Against Risk in an Era of Escalating Cyber Threats

The Economics of Defense: Modeling Security Investments Against Risk in an Era of Escalating Cyber Threats

New Juniper Networks-sponsored research, by the RAND Corporation, "The Defender's Dilemma: Charting a Course Toward Cybersecurity," introduces a first-of-its-kind heuristic model that helps companies map the economic drivers and challenges of defense.

Cyber-attacks are rapidly becoming one of the largest corporate risks that companies in all sectors face. From the loss of intellectual property due to corporate espionage to alarmingly common large-scale data breaches, it is clear that companies must do more to get ahead of threats and effectively manage risks. In response, companies have focused significant time, energy and resources to stop the threats posed by the attacks they face.

This focus is for good reason. A Juniper Networks-sponsored study from the RAND Corporation (RAND) last year, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," found that attackers have organized cyber black markets that are now at unprecedented levels of economic maturity. In practice, these markets are making attackers much more efficient in penetrating corporate networks and providing greater profits. In fact, the research predicted that the ability to attack will soon outpace the ability to defend.

> Juniper strongly believes that while the economic calculus for attackers is clear, the same cannot be said for companies who face a much more hectic, unclear and chaotic landscape.

Report Key Findings:

Juniper believes RAND's new model identified five main drivers that influence the costs of cybersecurity to companies detailed in this summary and RAND's full report. Each currently or will have a significant impact on cost.

1. There is No One-Size-Fits-All: Companies are Not Taking an Optimal Investment Strategy
2. Many Security Tools Have a Half-Life and Lose Value
3. The People Imperative: Investing in the Workforce Leads to Less Costs Over Time
4. The Internet of Things is at a Crossroads
5. Eliminating Software Vulnerabilities Leads to Major Cost Reductions

While many in the security industry have known for some time that these drivers are important to consider anecdotally as part of a security program, for the first time RAND's research quantitatively models the impact they have on cost. By doing so, this new model helps provide data-driven insights to understand why each driver matters and how they can enable companies to more strategically and holistically manage security risk.

The Defender's Dilemma

RAND's new research, which looks at the economic realities for defenders, suggests that chief information security officers (CISOs) feel they are treading water at best—investing more money in security without feeling any more secure. Even more concerning, they believe that attackers are quickly gaining on defenders and many are not sure about if or when they have invested enough in security.

This dynamic is in part caused by the continued lack of progress in understanding cybersecurity as an enterprise risk by many companies and even the security industry itself. Managing risk is often a misunderstood term in cybersecurity; focused on risks posed by threats and vulnerabilities instead of risks to business outcomes and operations. Often times, much of the emphasis—and even the metrics used to demonstrate the value of security programs—is on the prowess of a particular tool or program to stop a certain number of attacks rather than metrics that matter more to the business.

Instead of measuring the volume of blocked attacks, the goal of a comprehensive security program should be to understand the return on managing risk to investment or reduction of risk on investment (RROI). This means finding better ways to understand the factors that most influence the total cost of cybersecurity risk and how they can be more efficiently managed.

To start to address this need, Juniper Networks engaged and sponsored economists and security experts at RAND to conduct research that explores the major factors that influence the cost of cybersecurity risk to organizations. The research also examines the investments organizations can make to more effectively manage the risks to their reputation, information and networks from the increasing threat of attacks.

RAND has a proven track record of providing objective analysis and insights that have helped other sectors navigate the challenging issues they face—from controlling healthcare spending to addressing national security conflicts and defense spending. Having the organization examine the pressing problem of the cost of cybersecurity to business will help the security community and practitioners validate many of the challenges they face and make stronger arguments to the C-suite about how to address this issue.

A Heuristic Model for Enterprise Security Risk

Key to RAND's efforts was the development of a first-of-its-kind heuristic model that provides companies with a learning tool to better understand the major factors that influence the costs of managing security risk and the various investment decisions that can impact costs. By observing how these factors might interact, the model provides a framework for thinking about cybersecurity choices differently.

While there are several valuable existing security risk models, such as Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) and Factor Analysis of Information Risk (FAIR), which help companies access specific risks they face and what information is most critical to protect, RAND's model is the first framework that starts to map the *holistic* cost of managing cybersecurity risk. It does so by looking at how different choices made by companies, combined with the introduction of new technologies and the actions of attackers, all interact and influence the costs of cybersecurity.

To obtain a holistic picture of risk, RAND's model examines the ways organizations seek to minimize the total cost of cybersecurity. This includes both the direct and indirect costs to organizations to prevent cyber-attacks, as well as the potential losses due to a successful attack, measured by the value of information at risk and the probability of a successful attack.

> RAND's model is the first framework that starts to map the *holistic* cost of managing cybersecurity risk

To determine the cost to an organization, RAND's model has 27 parameters that influence the cost to an organization over a 10-year period. Each is adjustable to see the impact it has on cost.

The parameters generally fall into three categories:

1. **Organizational Characteristics:** The size of an organization, number of computers/devices in the network and the value of information at risk.
2. **Security Program and Investments:** Model allows companies to make decisions about the use of four different instruments, each that have costs but also reduce the possibility of a successful attack:
   - Direct costs of buying and using security tools
   - Direct and indirect costs of conducting advanced training of employees about threats
   - Indirect costs due to losses in potential productivity associated with restrictions on smart devices and air-gapping particularly sensitive subnetworks
   - The diligence of security staff to execute security programs
3. **Changes to the Ecosystem:** How changes in the technology ecosystem can influence the cost of security. For example, how the introduction of more devices with the Internet of Things (IoT) changes the attack surface or how number of software vulnerabilities introduced in a given year influences the likelihood of a successful attack and subsequent cost

In practice, Juniper believes that the model provides a systematic starting point to help CISOs understand the different decisions they can make to protect their organizations and better engage and garner support from the broader C-suite.

> The model provides a systematic starting point to help CISOs understand the different decisions they can make to protect their organizations and better engage and garner support from the broader C-suite.

To that end, Juniper created an interactive interpretation of the model that allows companies to apply many of the parameters to their organization. It allows users to change the major variables that have the largest influence on cost and begin to determine the proper mix of security investments companies should consider going forward.

Ultimately, the model's projections are directional versus diagnostic, as each company will have their own unique needs and challenges. However, this provides a strong starting point and discussion tool for security professionals looking to garner more support in their organization.

For companies and policymakers interested in exploring the model in its entirety, the methodology of RAND's full model is available in the appendix of the full report.

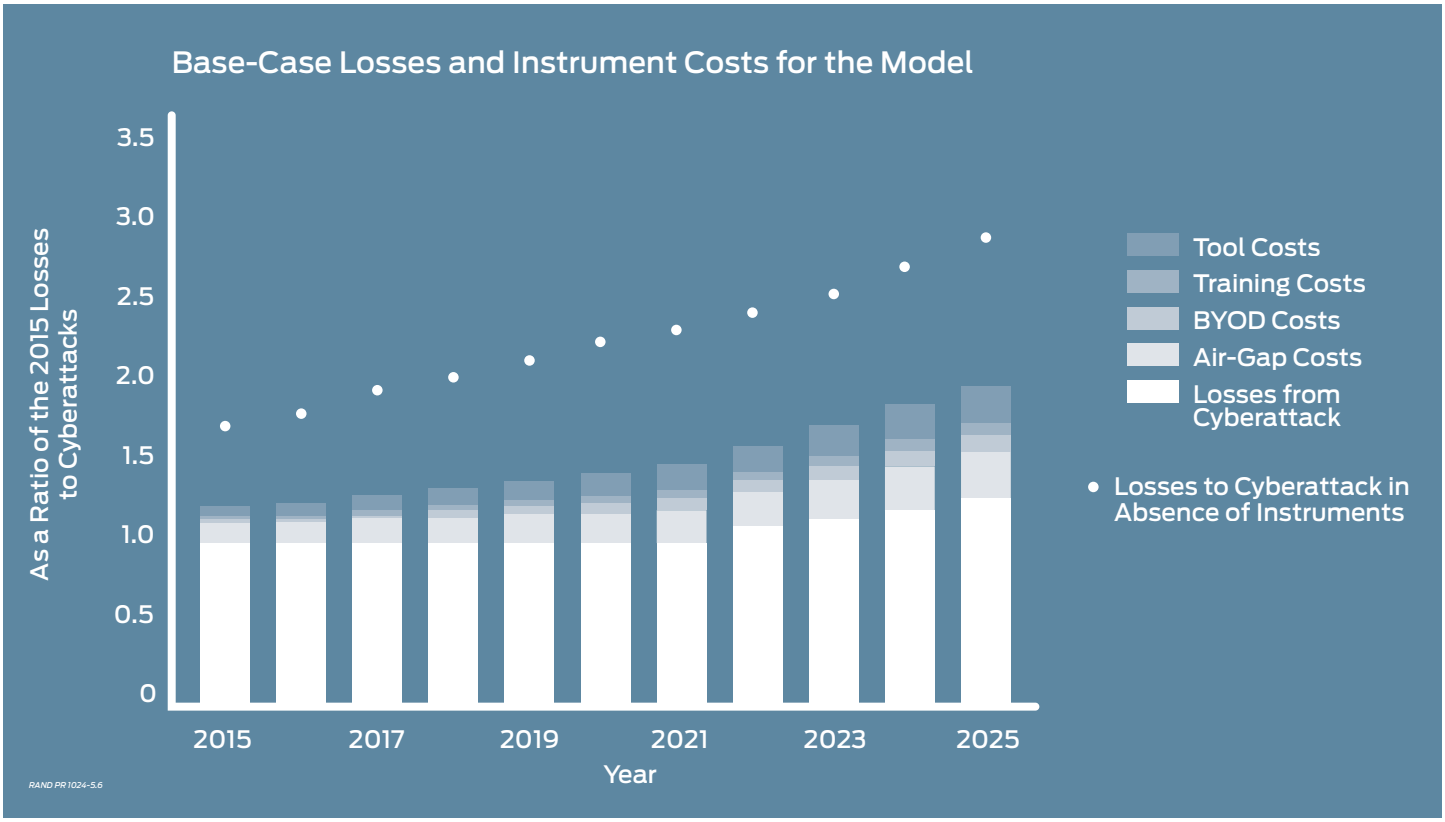
What the Model Tells Us About the Course of Security

Even more important than how the model works are the insights that it produces. RAND's report details a baseline case using the model, which looks at costs across the entire corporate world and how they change over the 10 years that the model runs.

RAND's model suggests that the cost of managing cybersecurity risk is set to increase 38 percent over the next 10 years across all businesses.

> The cost of managing cybersecurity risk is set to increase 38 percent over the next 10 years across all businesses.

Interestingly, most of the cost increase is not due to the rise in losses from cyber-attacks themselves; rather, it is from the increasing costs of security programs (e.g., investing in tools and training, restricting Bring Your Own Device (BYOD)/smart devices and air-gapping the network) to companies as they look to control potential losses. However, these investments are ultimately cost-effective because the losses without the investment would be much greater and rise more quickly. In the below chart, the dotted line shows how much losses would have been if companies did not invest in protecting their networks.



Major Cost Factors for Chief Information Security Officers

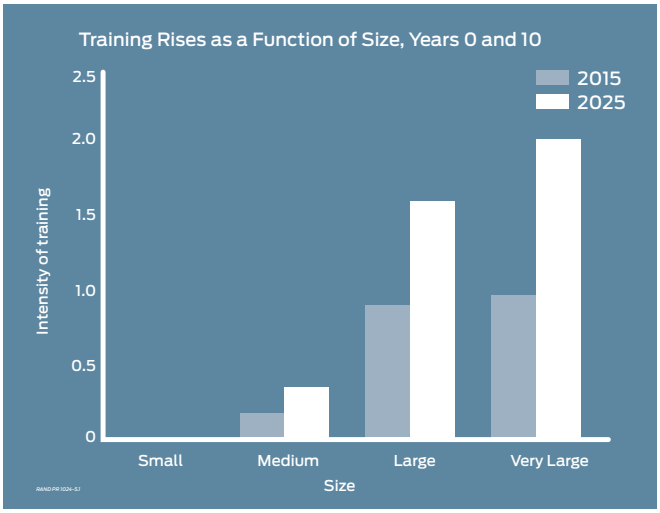
RAND's model also provides valuable insights for businesses. Juniper believes there are five major cost factors confirmed by the RAND model that must be taken into consideration as businesses evolve their security postures. While these factors are known by many in the security community to be anecdotally true, their high economic impact in RAND's model confirms their significance.

1. There is No One-Size-Fits-All: Companies are Not Taking an Optimal Investment Strategy

RAND's research suggests that many companies are likely not taking the optimal economic strategy with their investments. The optimal number of security tools, training for employees, restrictions on personal devices and decisions on which networks need to be segmented from the Internet, varies greatly from company to company.

Small and Medium-Sized Businesses

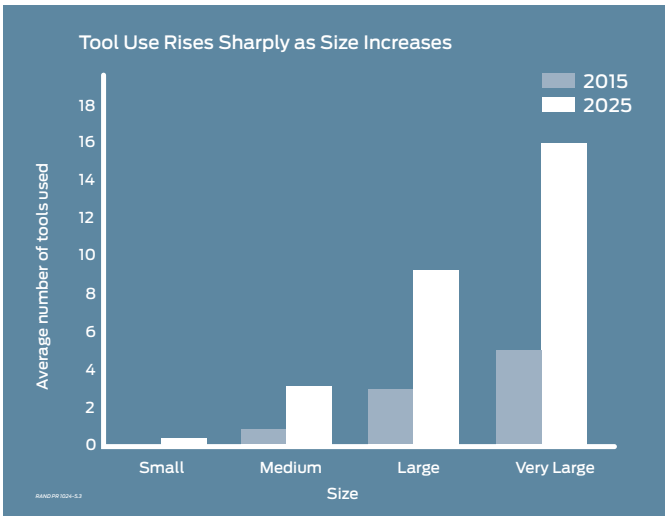
Small and medium-sized businesses (SMBs) benefit most from basic tools and policies, while not overinvesting in complex security trainings and more advanced security technologies. Because SMBs have a much smaller attack surface and are less likely to face a sophisticated attacker, overinvesting in high-cost security investments would add a disproportionate cost when compared to the likelihood of a breach and the potential losses they would experience as a result. Instead, basic tools and policies help to best protect SMBs by securing the network and restricting the use of personal devices on it.



Large Organizations and High-Value Targets

On the other hand, large organizations and/or those with highly sensitive information, such as defense contractors or organizations with significant amounts of intellectual property, require investments in a full range of policies and tools. The likelihood that they will be targeted by an advanced attack, experience a higher volume of daily attacks or face some type of intrusion is much greater. If significant investments are not made, then losses endured due to an incident would be huge.

Further, larger companies are likely able to benefit from economies of scale with their security investments. For example, providing advanced security training becomes more cost-effective per individual as the number of employees increases.



Assumes basic security awareness training and out of the box tools are in place.

2. Many Security Tools Have a Half-Life and Lose Value

One of the most challenging issues facing companies is the countermeasures attackers use to evade defenses. Attackers are constantly developing countermeasures to new security technologies, which limits the relative effectiveness of those tools over time and requires companies to invest in new technologies to take their place.

Take detection systems like sandboxing or anti-virus, for example. While very valuable when first released and a necessary part of the security equation for large organizations, these types of defenses are prone to countermeasures. Hence, they must be constantly re-evaluated and new solutions need to be put in place for defenses to remain effective against attackers. Measures beget countermeasures (the adversarial dynamic) pretty much sums up the root cause of cyber buildup.

This buildup ultimately drives up the amount companies must spend on security technologies to maintain similar levels of protection. It also increases operational costs to companies, which often find themselves with an increasingly diverse set of security technologies that need to be managed by security teams.

RAND's model projects that over time *the effectiveness of these technologies that face countermeasures falls by 65 percent over 10 years*. As a result, the overall amount companies should spend on security tools as a proportion to the overall cost of security to the organization goes up 16.2 percent when comparing the amount spent in the first and final year the model runs. This number may seem small to some out of context, but considering tools are the single largest cost of security to companies, the increase would be significant in real dollars.

So where should companies focus their investments? RAND also found that certain types of security tools are not prone to the problem of countermeasures. Technologies and security functions focused on improving security and patch management, automation and improving policy enforcement across the corporate network fall into this category because they are not the types of tools that attackers will try to get around.

Ultimately, most companies will need a mixture of tools that fall into both categories to protect their systems. However, Juniper believes what is most important is that companies understand that this dynamic exists and keep it in mind as they evaluate new investments.

Prone to Countermeasures

- Anomaly detection
- Signature detection
- Sandboxing malware
- Hack-backs
- Anti-phishing training

Less Prone to Countermeasures

- Firewall policy enforcement and automation
- Multi-factor authentication
- Automated patch management and patch version monitoring
- Sub-network isolation
- Network access control

3. The People Imperative: Investing in the Workforce Leads to Less Costs Over Time

One of the factors that RAND's model suggests could significantly reduce security costs over time is the investment in training as well as building a diligent security staff. A well-staffed and knowledgeable security team is equally if not more important than investing in new tools. The best tools are not going to be effective if not properly managed, which is taken into consideration in the model.

According to the RAND model, *companies with high diligence—those with the most effective security and IT staff at managing security programs—are able to curb the cost of cybersecurity by 19 percent in the first year and 28 percent by the tenth year that the model runs,* when compared to organizations with very low diligence.

Juniper believes, while there is certainly a shortage of knowledgeable security professionals today, these potential savings are too large to ignore. Companies need to be very aggressive in investing in training and expanding security teams. If new staff is not possible, another potential approach is outsourcing specialized security functions to other experts. RAND's report suggests leveraging managed services can provide benefits:

> *Many defenders choose to outsource some important defensive functions to specialists who can provide a particular service to a wider range of customers. For example, many large organizations do not conduct their own network penetration testing because the discipline is so specialized that it is difficult to hire and maintain native staff capabilities at the highest levels of capability.*[1]

2015

Diligence Level	Difference in Costs of Attack
Very Low	13% Increase
Low	10% Increase
Medium	Neutral
High	Neutral
Very High	6% Decrease

2025

Diligence Level	Difference in Costs of Attack
Very Low	18% Increase
Low	13% Increase
Medium	Neutral
High	6% Decrease
Very High	10% Decrease

[1] "The Defender's Dilemma: Charting a Course Toward Cybersecurity," RAND Corporation, 2015, Martin Libicki, Lillian Ablon and Timothy Webb.

4. The Internet of Things is at a Crossroads

There is a lot of talk about IoT, including a lot of hype. But one thing is clear: companies will have more devices hitting their networks than ever before in the near future. According to RAND, IoT will have an impact on overall security costs; however, it is unclear if it will be positive or negative. Juniper believes this puts organizations at a crossroads.

If companies are able to properly deal with the security implications of IoT by applying security technologies and device management in a smart and sophisticated way, they could see savings in the long run as the number of devices in the network outnumber PCs. On the other hand, if IoT follows a similar path that plagued the early PC days, with a myriad of security issues, companies will face skyrocketing security costs.

In the latter scenario, RAND's model suggests that the introduction of IoT would increase the losses that companies experience due to cyber-attacks by 30 percent over the course of 10 years.

While most companies are a few years away from experiencing the true impact of IoT, Juniper believes companies should start carefully considering how they will incorporate these devices into their security programs and networks now. Companies will need to ensure that the performance of their security infrastructure is capable of managing the increased bandwidth that will come with these new devices and connections.

Further, companies will need to determine which security controls should be put in place to govern these new devices being introduced into the corporate environment. Similar to how BYOD is being managed today, companies must ensure now that they have the proper tools to quickly provision and manage new IoT connections as they enter their networks in the near future. This includes establishing and enforcing proper rights management to ensure these new devices do not increase the attack surface, as well as establishing clear corporate policies on employee use of personal IoT devices in the workplace.

5. Eliminating Software Vulnerabilities Leads to Major Cost Reductions

One area that RAND identifies as having a massive influence on cost is the number of exploitable vulnerabilities in the software and applications they use. Companies often find themselves having to invest in defensive measures because foundational systems and software are unsecure. Unfortunately, this particular indicator is also largely out of the control of the CISO and dependent on software makers to build more secure code.

RAND's model found that if the frequency of software vulnerabilities is reduced by half, the overall cost of cybersecurity to companies would decrease by 25 percent.

Yet, the likelihood that software vulnerabilities will be less frequent in the future is doubtful. If network and software architectures were static, defenders would eventually gain the upper hand—but innovation is the lifeblood of the information technology sector.

RAND's research suggests that the number of new vulnerabilities is likely to increase with the proliferation of devices brought on by IoT and the growing complexity of software ecosystems built on previous versions of code.

The good news is there is much work being done in the industry to improve software quality. For example, there are free tools available to developers that help them identify vulnerabilities before shipping products. As more software makers use these tools, the number of vulnerabilities being discovered in products is likely to drop.

Juniper believes it is also incumbent on companies to scrutinize the software they are using and demand better security testing and patching by software providers. If poor security leads companies to stop using a certain program, software makers will have a much stronger incentive to deliver higher quality products with less vulnerabilities.

A Path Forward For Companies and the Industry

So what can companies do to better manage their security investments against risk in an era of escalating cyber threats?

Manage the Security Portfolio like a Business

Companies must find a better way to manage security like a business—quantifying the risks and benefits of different decisions. Juniper believes that RAND's model provides several actionable insights that companies should consider as they evaluate their security posture and spending.

Ultimately, CISOs should strive to have better metrics to determine RROI. In short, companies need to constantly evaluate the lifecycle and effectiveness of their programs —just as one would manage a stock portfolio for their business. This is where Juniper's interactive interpretation of the model and RAND's full model and methodology are helpful in determining which tools are most effective to accommodate different companies' unique needs.

For more information on Juniper's work and investments in security, visit here.

Evaluate Security Tools with Countermeasures in Mind

According to RAND's findings, "organizational choices can, and perhaps should, be influenced by the likelihood of countermeasures to whatever investment is made, notably in systemic defenses... Corporations should think about installing measures of the sort that are less likely to attract countermeasures."

Juniper believes this means companies should prioritize investments in tools that automate security tasks through a centralized management and distributed enforcement platform, especially when securing networks. Automation is a major area of focus for Juniper and there are several reasons why we encourage our customers to consider investments in automation tools:

- Tools with built-in automation are less prone to countermeasures, making them less likely to lose effectiveness over time and maintain their value.
- Automation can reduce other security costs to organizations by lessening the operational demands on already stretched IT teams.
- Automation allows security staff to spend less time configuring and testing systems, enabling them to focus more attention on other essential tasks like mitigating the most sophisticated attacks they face and making new additions to their defensive posture.
- Finally, having a centralized system can help increase the benefit of other security investments by making them easier to manage and execute. For example, automated and centralized management of threat detection feeds provides a way to quickly push what is often a patchwork of different sources of threat information to enforcement points across the network.

The Need for Industry Action

Making systematic progress on security must not sit on the shoulders of CISOs alone. Juniper believes it is imperative for the broader security industry and government to take important steps to change the current dynamic and tip the scale toward defenders.

Train the Next Generation

The key to getting in front of attackers is training the next generation of developers to do a better job securing the innovations they create. RAND's report also supports this notion, stating that "...secure coding is not part of the standard curriculum for computer science majors. These students are the next generation of people developing and creating the devices."

If the next generation can be trained to create inherently more secure software, the potential for compromise could be drastically reduced, which could lower the overall cost of security for companies.

Training students on security will also mean that more of the next generation will become security professionals and be more effective in those roles. By creating a pipeline now, the security industry will finally be able to get ahead of the current lack of trained professionals. In addition, by learning about the ethics of hacking, many future hackers that might be tempted to participate in the black market would more likely use their security skills for good.

Develop Technology with Countermeasures in Mind

Further, security innovators, like Juniper, must continue to create security technologies designed to withstand the countermeasures of attackers and improve visibility and control over the network. While the cat and mouse game between attackers and defenders will exist until the end of time, a more concerted effort to address this reality could slow the pace of attackers against new technologies.

We are not claiming that this report or model provides an end-state for understanding cybersecurity risk. It should be the beginning of a discussion that the security industry must have about how it understands risk. We hope that our work with RAND helps move forward and prompts further discussion.

The full report from the RAND Corporation, as well as last year's report and supplemental materials from Juniper, can be found here.

About the Report

"The Defender's Dilemma: Charting a Course Toward Cybersecurity," is authored by RAND Corporation security experts, Martin Libicki, Lillian Ablon and Timothy Webb. It is based on in-depth interviews conducted between October 2013 and August 2014 with CISOs on the current and emerging threat landscape. This research builds on the first report of a two-part series sponsored by Juniper from RAND, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," which examined the economic drivers for attackers and the sophisticated underground black market they've created to scale their efforts.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
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

JUNIPER NETWORKS

Juniper Networks (NYSE: JNPR) delivers innovation across routing, switching and security. Juniper Networks' innovations in software, silicon and systems transform the experience and economics of networking. Additional information can be found at Juniper Networks (www.juniper.net) or connect with Juniper on Twitter and Facebook.