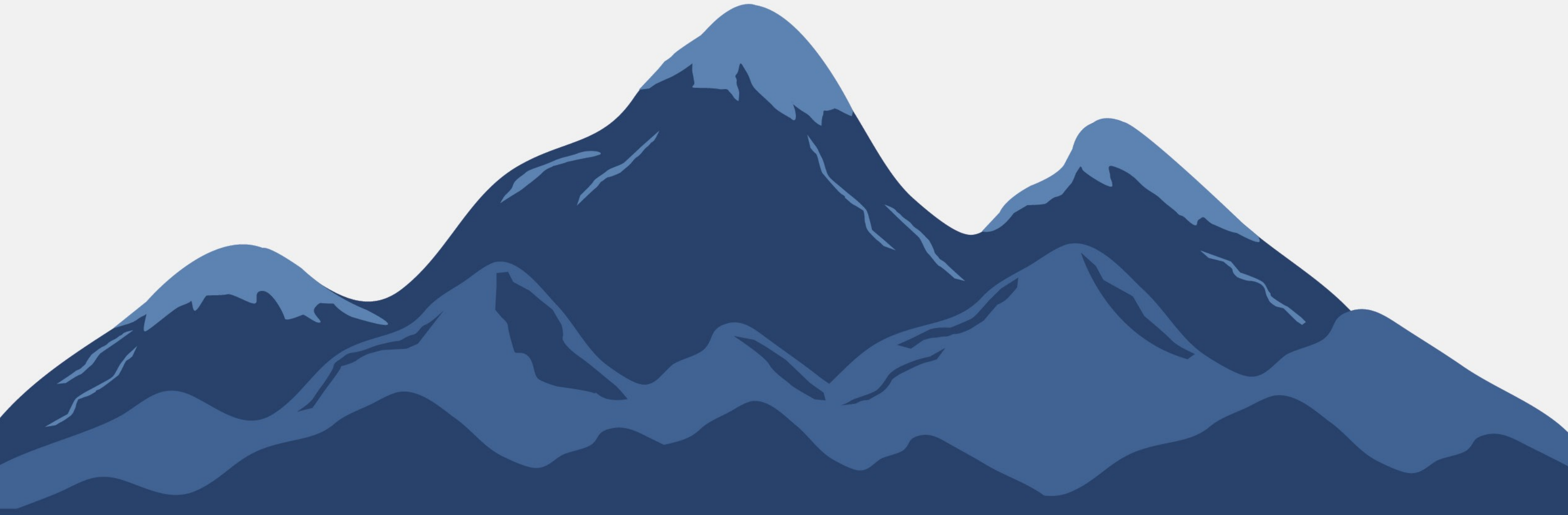
FROST & SULLIVAN



A View From the Top

The (ISC)² Global Information Security Workforce Study CXO Report

A whitepaper derived from the (ISC)² Global Information Security Workforce Study, a Frost & Sullivan market study, in partnership with:

(ISC)²®

Booz | Allen | Hamilton
strategy and technology consultants

Prepared by
Michael Suby
Global Program Director
Information Security

www.frost.com

INTRODUCTION

These are turbulent and paradoxical times for Chief Security Officers (CSOs) and other executives with security and regulatory compliance responsibilities in their bailiwick. There are five primary factors contributing to this combination of turbulence and paradox:

First, there is no slowing in the amount of data that must be secured, and the places where that data resides—statically and on a transient basis (e.g., on consumer-owned devices, in the cloud, on portable media, and in company-owned data centers). In other words, the perimeter is fluid, and the footprint to secure is expanding boundlessly. Paradoxically, clamping down on data security is counter to the data fluidity that end users and their organizations demand and expect.

Second, electronic operations are mission-critical for many public and private organizations. Disruptions in external- and internal-facing systems and applications can produce a tsunami effect. Adding to the potential for disruptions is the on-going feature and functionality race, frequently accomplished without a full understanding of the security risks. Security, consequently, is an after-the-fact consideration in application development. Yet, bringing security into the forefront of application development is a costly anchor in this feature and functionality race.

Third, the threat actors continue to evolve in stealth, organization, and sophistication. They are, simply, foes that are constantly re-arming themselves with new weapons. Increasingly, the most significant threat to an organization is what it does not know or cannot detect.

Fourth, regulatory obligations are increasing. The previously stated factors of an expanding risk footprint, susceptible electronic operations, and an untiring foe drive the call for more, not less, regulation. But exclusively focusing on the chapter and verse of regulations is akin to providing cyber criminals with the “how to” security playbook.

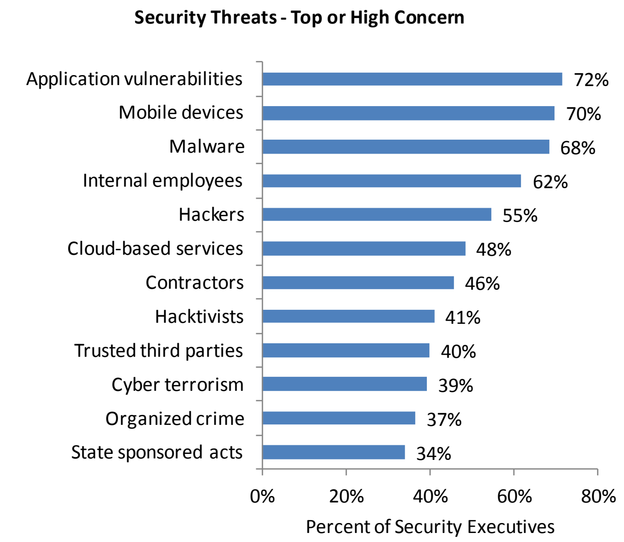
Fifth, locating and hiring skilled and experienced information security personnel is a perennial challenge. While the education system has contributed to students’ ability to leverage new information technologies—systems, devices, and applications—the focus on security has been limited. Consequently, the development cost to build a security-conscious and -knowledgeable workforce falls on their future employers.

Through it all, CSOs and other security executives gravitate to this turbulent and paradox-lessening role. In a late 2012 global survey of 12,396 information security professionals, which included 1,634 with security executive titles, 82 percent of the security executives stated they are somewhat or very satisfied with their current roles. Most have made it a career; the average security executive duration in the security discipline is over 14 years. Plus, annual base compensation is over $150,000 for nearly one-third of security executives in private industry, with approximately two-thirds stating they received a pay increase over the last 12 months.

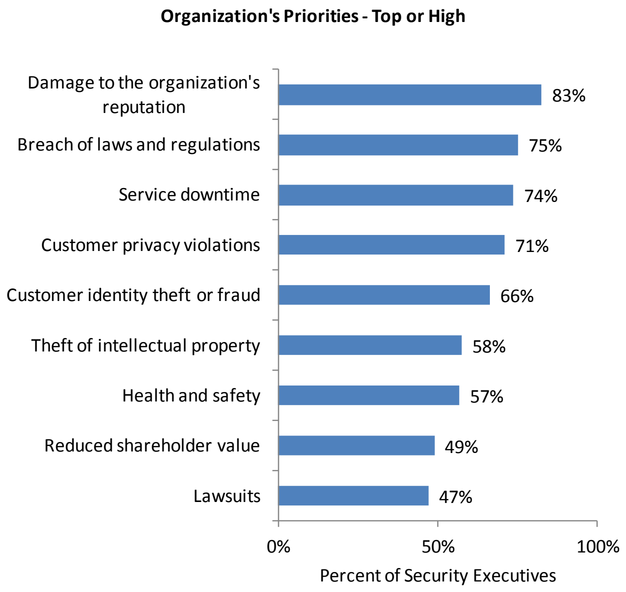
Considering the volume, diversity, and uncertainty of security challenges facing executive security professionals, defining priorities is essential. In this paper, we examine the priorities of security executives, the constraints they are encountering, and offer our opinion on how the role of security executives is changing.

THREATS, PRIORITIES, AND TIME

Security executives have earned their positions by making good and balanced decisions on priorities and where to devote their time, as well as having a keen sense of the security threats that pose the greatest risk to their organizations. According to security executives, nearly three-quarters consider application vulnerabilities as the greatest security threat, followed by mobile devices, and then malware. Variation is expected across organizations. For example, the hacker threat rises to the top three for security executives in the IT industry; and security executives in government-defense view cyber terrorism and state-sponsored acts as the top two threats.



Priorities—or more aptly stated, the outcomes—to avoid follow a consistent theme of protecting private and sensitive information. Additionally, service downtime was in the top three "to avoid" priorities among security executives. Again, security executives vary in perspective, with the largest deviation being in government-defense, where service downtime shared the top spot with damage to the organization's reputation. Proportionately, but not surprisingly, given the nature of their businesses, a higher percent of security executives in the banking, insurance, and finance sectors rated data protection priorities higher than security executives in other industries.

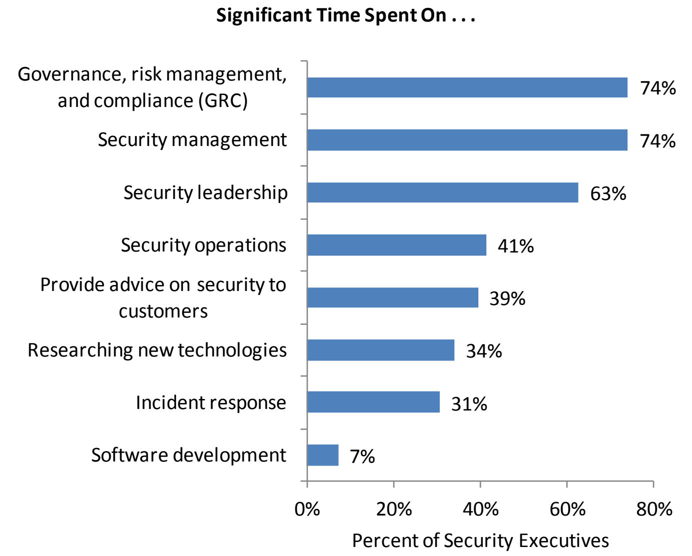


Focusing on where security executives devote significant portions of their time, three areas dominate: governance, risk management, and compliance (GRC); security management; and security leadership (see chart on next page). Variation, again, was apparent in the finance, banking, and insurance sectors, and was also based on company size. For security executives with organizations of more than 10,000 employees, or in the finance, banking, and insurance

The increasingly complex nature of cyber security issues, intermixed with geopolitical issues, is making cyber risks even more unpredictable and more difficult to address. In this regards, more preparatory work to detect and respond to new/emerging risk issues (in alignment with business changes) will be critical.

Dr. Meng Chow Kang, CISSP, CISA
Director for Information Security for China and AP
Cisco Systems

sectors, GRC occupied a decidedly higher position, with 84 percent of the security executives stating they spent significant time on this activity. Drilling deeper into these three high-level activities, the top two activities selected as top or high priority by security executives are shown within each activity category:



- **GRC** – Developing internal security policies, standards, and procedures (78 percent); and auditing IT security compliance (63 percent) were the top two activities within GRC.
- **Security management** – The top two "significant time" activities in security management were inter-departmental activities and cooperation (64 percent); and manage internal information security awareness programs (63 percent). Reflecting the challenges that come with size, inter-departmental activities and cooperation was chosen by 69 percent of security executives in organizations with more than 10,000 employees; and internal or political issues rose to second (63 percent).
- **Security leadership** – Besides security leadership and management (chosen by 94 percent as an activity that consumes significant time), security compliance management was the next highest, at 63 percent. Also, three-quarters of security executives in banking, finance, and insurance sectors, as well as both categories of government defense and non-defense, chose security compliance management within their security leadership role as an activity consuming significant time.

MANAGING SECURITY RISKS: PEOPLE, PROCESS, AND TECHNOLOGY

A clear signal from security executives is that security personnel are essential in managing security risk. In a separate survey question on whether the respondents were involved in hiring, nearly two-thirds of security executives stated they were. Participation is greatest with security executives employed in private industry: 72 percent are involved in hiring, as compared to just 51 percent of government-employed security executives. Reflecting the security executives' greater hands-on involvement in smaller organizations, the percentage of security executives involved in hiring was highest with private (non-government) organizations with less than 500 employees (80 percent); and dropped to 60 percent with security executives in private industry organizations with more than 10,000 employees.

Attracting and retaining quality professionals is a vital skill. Those professionals who combine business intimacy with an up to date security toolkit need to be actively developed and mentored. Education must also consider the 'asymmetric' nature of working today, and assist employees to understand and mitigate the risks arising from remote working and mobility.

Sarah Bynum CISSP, CPP
Director of Security
Siemens Energy, Inc.

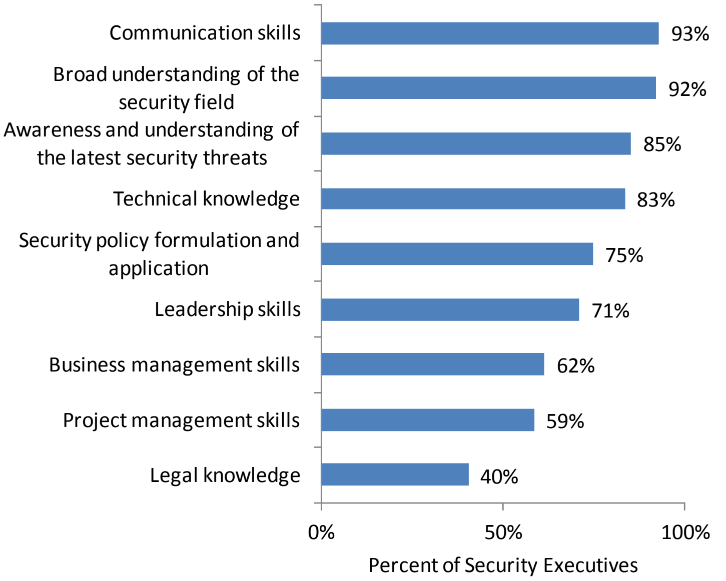
Recognizing that managing security risk requires a combination of people, process, and technology, it is interesting to note that a majority of security executives indicated that a significant amount of their time is spent in "process" activities, such as: developing internal security policies, standards, and procedures; inter-departmental coordination; and internal security awareness programs. By contrast, the percent of security executives indicating they spend a significant amount of time in researching new security technologies was 34 percent.

In a deeper examination into security personnel, the majority of security executives state they have too few security personnel. Most pronounced is government security executives—77 percent state their organizations have too few security personnel, compared to 63 percent of security executives in private industry. Business conditions were cited as the number one restraint in hiring more security personnel (chosen by 61 percent of security executives).

When asked about the attributes of successful security personnel, security executives view general business and organizational skills to be of nearly equal importance to knowledge and technical skills in the security discipline. Incidentally, the rank and file expressed a similar view.

Given the dynamic nature of security, training is essential to gain the most from existing security personnel. To that end, 59 percent of security executives and 49 percent of rank-and-file believe their organizations have invested adequately to provide the training they need. Consistent with the prioritized listing of security threats, a majority of security executives stated that training on cloud computing (57 percent), bring-your-own-device or BYOD (56 percent), and information risk management (53 percent) should be provided.

Attributes of a Successful Security Professional (Important or Highly Important)

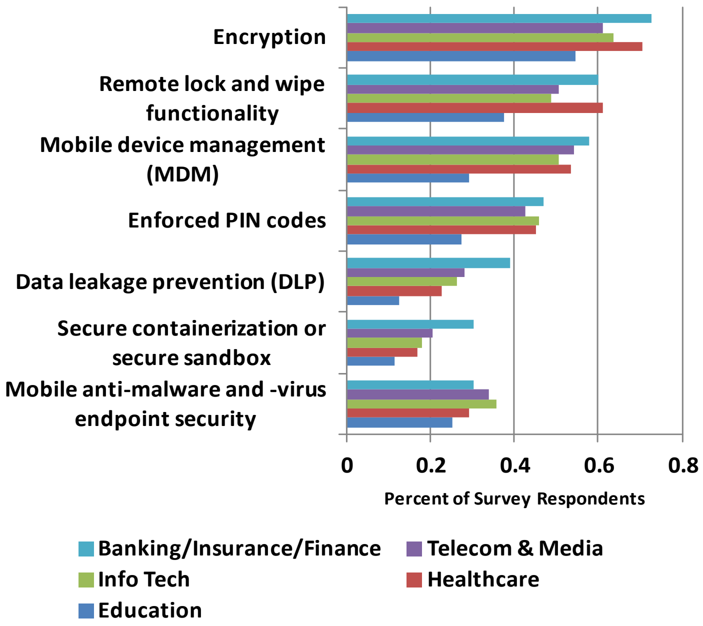


While 35 percent of security executives predict that spending on personnel will increase over the next 12 months (37 percent in private industry and 26 percent in government), and 31 percent predict a spending increase in training and certification (33 percent in private industry and 24 percent in government), this is still insufficient to fill the personnel gap for approximately one-third of security executives. Spending increases in professional, outsourcing, and managed services is predicted by approximately 30 percent of the security executives (again, greater in private industry than government).

Most of the ISO/CISO must cope with the increasing threat landscape (e.g. BYOD, xaaS, Big Data) and reporting requirements internally and externally. The only escape to the Catch-22 situation is to formalize and automate needed processes. To achieve the requirements many more experienced and trained people are needed. But they do not exist and will be difficult to recruit. Organizations like (ISC)² are well suited to fulfill the training and educational aspect for this demand.

Rainer Rehm, CISSP
Information Security Officer
MAN Munich

Differing Mobile Device Security Technologies in Use Among Select Industry Verticals



Spending on security technology is also expected to increase over the next 12 months, compared with spending on personnel and training. Thirty-nine percent of security executives (41 percent private industry and 31 percent government) predict a spending increase in security hardware and software. Some of that increased spending will be directed toward mitigating the security risks associated with BYOD, of which a wide range of security technologies are in use. Other security technologies that security executives cite as providing significant improvements to system and network security are:

- Network monitoring and intelligence (74 percent)
- Intrusion detection and prevention (70 percent)

Increased spending in these technologies is consistent with the security threats of most concern to security executives (see chart on page 2). Understanding network behaviors, with high fidelity and speed, whether the threatening behaviors are internally generated or external, is part of the prevailing trend in next-generation firewalls and intrusion detection systems; and in the evolution in security information and event management (SIEM) systems—increasing depths of contextual awareness and scalability.

A missing element in security executive attention and spending is proactively addressing application vulnerabilities. From the first chart in this report, application vulnerabilities were cited by more security executives as a top or high concern than all other security threats. However, in the chart showing where security executives are spending their time (page 3), software development was the lowest (only seven percent of security executives stated they spend significant time on software development). A similar result was found with the rank-and-file—time spent on secure software development is a low priority activity; and certifications in secure software development is also low relative to other types of security certification. It could likely be that the predominant approach to mitigating the risk associated with application vulnerabilities is reactive—detect when an exploit is occurring (e.g., the exfiltration of sensitive data)—rather than discover and fix vulnerable code before the code is placed in operation. This conclusion is consistent with the previously stated security technology spending—that is, technologies designed to detect anomalous behaviors.

Threat trends today are becoming more sophisticated, stealthy and more organized. Unfortunately, we have been fighting against those threats individually, not in an organized fashion. In order for us to change the status quo, CSOs need to understand that developing the appropriate individual countermeasures is a pressing matter; while at the same time working to build consorted and organized countermeasures to effectively protect the entire system is crucial as well. I have high hopes that CSOs with the vision to collaborate will enable CEOs and other stakeholders to grasp what needs to be done and take action.

Itsuro Nishimoto, CISSP
CTO, LAC Co., Ltd
Japan

THE LAST WORD

Managing information and network security risk is an informational intensive activity. More real-time data, data of high quality, and rapid but confident analysis has been and continues to be the lifeblood of security risk management. Long before "big data" became a high tech catch phrase, it was part of the security profession's arsenal.

Big data in the security discipline can and needs to improve significantly. But, in order to improve, CSOs must look beyond what they can do from within their organizations to what they can do better through collaboration with others. Two areas where we believe impact is possible are:

- ***Inter-company data sharing, analysis, and best practice strategies*** – Cyber criminals and other miscreants are increasingly driven by profit; and, with that, repeatable operations. Consequently, attacks perpetrated on one organization are likely being attempted on others—and, in many cases, with an aspect of customization. Collaboration among companies in the same industry is a viable approach to accelerate and improve threat detection and mitigation. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is an example of an industry forum that is already moving forward in this direction. Tapping into the data warehouse of national governments is another opportunity. Although private-public cooperation in cybersecurity is in its operational infancy, there is promise. The key to success will be in the development of methods and procedures in the efficient and high-fidelity exchanging of threat information.
- ***Outsourcing*** – More and better data is not the end-all in uplifting cybersecurity. Expertise, experience, and efficient processes are also essential. However, as our survey confirms, talent is in short supply. Plus, in-house security personnel have a structural bias—they primarily focus on the circumstances of their own organizations. While understandable, there is value in tapping the expertise of organizations that engage in security issues across multiple organizations and industries. Consequently, and as our survey confirmed, nearly one-third of security executives are expected to increase their spending on professional and managed security services. Our projection is that this trend will intensify in the years ahead, with organizations taking a hybrid approach of in-house and outsourcing. In hybrid, organizations will retain in-house the most sensitive aspects of their business operations, and outsource recurring cross-industry security operations and less frequent but talent-deep security projects (e.g., vulnerability assessments) to professional and managed security firms.

Information and network security needs to constantly re-invent itself across all three operational pillars—personnel, processes, and technology. At the top, CSOs are charged with making balanced decisions on where and how much to invest in each of these pillars, and locating ways to lessen the security paradox (i.e., elevating security without hindering business priorities). In our view, collaboration and outsourcing must become a larger share of how security is done.

Michael Suby

VP of Research
Stratecast | Frost & Sullivan
msuby@stratecast.com

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT (ISC)^2 AND THE (ISC)^2 FOUNDATION

(ISC)^2 is the largest not-for-profit membership body of certified information security professionals worldwide, with nearly 90,000 members in more than 135 countries. (ISC)^2’s certifications are among the first information technology credentials to meet the stringent requirements of ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)^2 also offers education programs and services based on its CBK®, a compendium of information security topics. The (ISC)^2 Foundation is the charitable trust of (ISC)^2, aiming to make the cyber world a safer place for everyone with community education, scholarships and industry research like the (ISC)^2 Global Information Security Workforce Study. More information is available at **www.isc2.org** and **www.isc2cares.org**.

ABOUT BOOZ ALLEN HAMILTON

Booz Allen Hamilton is a leading provider of management and technology consulting services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. Booz Allen is headquartered in McLean, Virginia, employs approximately 25,000 people, and had revenue of $5.86 billion for the 12 months ended March 31, 2012. To learn more, visit **www.boozallen.com**. (NYSE: BAH)

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today’s market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? **www.frost.com**

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Colombo
Delhi / NCR
Detroit
Dhaka
Dubai
Frankfurt
Hong Kong
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Manhattan
Mexico City
Miami
Milan
Moscow
Mumbai
Oxford
Paris
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw
Washington, DC