# 2020

# STATE OF GEORGIA'S INFORMATION SECURITY AND CYBERSECURITY ECOSYSTEM

TAG | Information Security

Driven by Innovation
Proven by Performance

# EXECUTIVE OVERVIEW

Welcome to the first iteration of the TAG Information Security and Cybersecurity Ecosystem Report. The purpose of this report is to highlight the robust information security ecosystem in the state of Georgia.

The Technology Association of Georgia (TAG) program "Where Georgia Leads" identifies the InfoSec community as one the leading contributors to Georgia's broader economy and puts Georgia at the forefront of the national conversation around technology.

As you will see in this report, the InfoSec ecosystem generates over $1.4 billion in annual revenue and is responsible for over 6,700 of jobs in Georgia. This innovative sector is a catalyst for the robust technology focused start-up community we are privileged to have in Georgia.

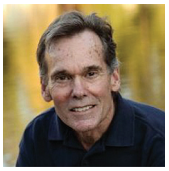
InfoSec and cybersecurity issues impact businesses and individuals every day. Based on industry studies, the average cost of a data breach globally is $3.92 million for 2019. This creates a strong demand for quality technology solutions. In fact, the worldwide market forecast for InfoSec and cybersecurity technology in 2019 is estimated to exceed $124 billion.

Many people in the Georgia InfoSec community contributed to this report and our desire is for it to be reflective of the broad spectrum of people, companies, and entities that make up this community. Whether in Atlanta, Augusta, Columbus, Savannah or many other cities in Georgia, InfoSec leads the way!

Going forward, we will continue to highlight the InfoSec community in Georgia, identify key trends and market drivers, and seek to be a resource for the community.

We sincerely hope that you enjoy this report. Thank you.

***Roy Hadley**, Special Counsel,*
*Adams and Reese LLP*
*Cyber Security and Privacy Practice,*
*Board Chair, TAG InfoSec Society*



***Don Campbell**, Managing Principal,*
*RightCourse, LLC*

***Contributors***

***Reba Adams**, Project Manager, Center for Economic Development Research, Enterprise Innovation Institute, Georgia Institute of Technology*

***Heather Maxfield**, Vice President of Government Relations and Statewide Activity, Technology Association of Georgia*

***Ahiliya Nat**, Georgia Tech Masters Student and TAG intern*

***Ken Rome**, Graphic Designer, Owner, Notusmedia*

***Carina Wingel**, Director of Marketing, Deposco*

# THE DYNAMIC GEORGIA INFOSEC TECHNOLOGY ECOSYSTEM

Information security (InfoSec) and cybersecurity are among the most scrutinized operational issues executives face today. And with good reason, the safety of an organization's data is sacrosanct. Organizations not doing a good job protecting its data will potentially face significant market consequences. Studies show that breached organizations lose significant revenues, as well as suffer the costs involved in recovery and remediation. Brand reputation is also inpacted.

In the first half of 2019, according to the ***Cyber Risk Analytics – 2019 Midyear Report***, there were more than 3,800 data breaches exposing over 4.1 billion records. This represents a 50 percent increase over the last four years. It's interesting to note that 89 percent of the breaches were the result of outside attacks.

*Effective data security is no longer an option, it is mandatory.*

The terms InfoSec and cybersecurity are often interchanged but there is a difference.

- Information security is focused on the security of data and information assets. InfoSec tools include a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information.

- Cybersecurity is the use of technology to prevent computers, servers, networks, and mobile devices from being attacked via the internet – hacked if you will.

According to the Georgia Department of Economic Development, Georgia serves as one of America's elite cybersecurity hubs, ranking No.3 in the nation for information security. More than 120 InfoSec companies call Georgia home and generate over $1.4 billion in revenue every year. Together, these companies employ over 6,700 network and computer system engineers and others across the state.

*If your role is information security, your focus is protecting your organization's data resources from any kind of unauthorized access.*

Georgia's vibrant InfoSec and cybersecurity ecosystem are innovative and robust. From founding father organizations such as Internet Security Systems (ISS), Secureworks and AirWatch to up-and-coming companies like Ionic, CloudStrike and Pindrop, the Georgia InfoSec ecosystem is leading the way in helping organizations and individuals protect their priceless data. See a listing of the Georgia-based InfoSec companies later in this report. Please note that the TAG Information Security Society has focused primarily on the companies that develop and deliver InfoSec technology in the form of software, firmware, hardware, and specialized on-demand services that protect data and networks from intrusion.

## Security Technology Spending to Grow

Worldwide spending on information security products and services reached more than $114 billion in 2018, an increase of 12.4 percent from 2017, according to the latest research from Gartner, Inc. In 2019, the market is forecast to grow 8.7 percent to $124 billion.

The National Association of Corporate Directors 2019 Public Company Governance Survey ranked cybersecurity threats as their 3rd largest issue effecting their business within the next 12 months (behind regulatory climate and economic slowdown). The survey found that 97percent of public companies and 94 percent of private companies are looking to improve cybersecurity oversite in the coming year.

A 2017 Gartner Group survey revealed that the top three drivers for security spending are:

- Security risks
- Business needs
- Industry changes

**Worldwide Security Spending by Segment, 2017-2019**
(Millions of U.S. Dollars)

| MARKET SEGMENT | 2017 | 2018 | 2019 |
|---|---|---|---|
| Application Security | 2,434 | 2,742 | 3,003 |
| Cloud Security | 185 | 304 | 459 |
| Data Security | 2,563 | 3,063 | 3,524 |
| Identity Access Management | 8,823 | 9,768 | 10,578 |
| Infrastructure Protection | 12,583 | 14,106 | 15,337 |
| Integrated Risk Management | 3,949 | 4,347 | 4,712 |
| Network Security Equipment | 10,911 | 12,427 | 13,321 |
| Other Information Security Software | 1,832 | 2,079 | 2,285 |
| Security Services | 52,315 | 58,920 | 64,237 |
| Consumer Security Software | 5,948 | 6,395 | 6,661 |
| **Total** | **101,544** | **114,152** | **124,116** |

Source: Gartner (August 2018)

A 2017 Gartner Group survey revealed that the top three drivers for security spending are:

- Security risks
- Business needs
- Industry changes

This simplified view of organizational needs can be greatly expanded as management drills down to the underlying causes. As we look out across the landscape, here are some of the mission critical factors that will help grow the InfoSec technology markets:

- **Increased Attacks on Small Businesses**

  Digital transformation implies that effective security is no longer an option, it is mandatory. Attacks will be spread out and a greater number of small businesses will fall within the radar of cybercriminals in 2020 and beyond. Small companies must re-assess their security posture and ensure adequate measures and controls are implemented to safeguard against today's cyber-attacks.

- **Large Organizations Cannot Rest Easy**

  While large organizations have already done considerable work to protect themselves from attacks, cyberthreats will get more and more sophisticated as cybercriminals look for new ways to break into networks and systems.

*Continued from page 2*

- **Automation will Drive Efficiencies**

  Organizations' use of automation and the use of technologies such as Robotic Process Automation (RPA) will increase. This will help with incident detention, analysis and response. Security Operations Centers (SOC) and incident response teams will need more automation to keep up with the pace of non-stop cyberattacks.

- **Businesses and Cybercriminals will Both Leverage AI, ML**

  Artificial Intelligence (AI) is taking center-stage in cybersecurity and includes the power of Machine Learning (ML), which has the potential to identify and respond to threats as they occur. This year, these technologies will get even more efficient at protecting customers, processing and prioritizing data and ascertaining which of the threats are real versus false alarms.

- **Hybrid IT Infrastructures Security will be a High Priority**

  Many organizations do not have centralized control and visibility of all the environments. This is due in part to the increased use of hybrid IT infrastructures that include cloud, third-party services and microservices. Security system integration and administrative dashboards will help provide the necessary flexibility and scalability.

*A recent study found that nearly 30% of all internet traffic comes from malicious bots. (2019 Forrester Research)*

Over the past decade data and network security needs have increased dramatically as organizations' information systems have taken on a hybrid nature, combining both in-house and cloud-based systems. According to research conducted by Secureworks, a cybersecurity company founded in Atlanta and purchased by Dell in 2011, organizations are behind the

*Continued on page 5*

## INFOSEC PRODUCT COMPANIES

Apptega
Arc Sight Inc
Barracuda
Blough Tech Inc
BMC Software Inc
Check Point Software Technologies
Clear Skies Security LLC
CodeGuard
Crossbeam Systems
Cyberscrub LLCC
Damballa Inc
Dataliant Inc
Dorian Software Creations Inc
EMC Corp/RSA Security
Giesecke & Devrient America
GeoTrust
IBM Internet Security Systems
Infineon Technologies
Intel
INTERNETSAFETY.COM Inc
Ipswitch Inc
IRONSCALES
Lancope
Liquidware Labs
Motorola AirDefense Solutions (Extreme Networks?)
nCircle Network Security LLC
Numerex Solutions LLC
Outpost Sentinel LLC
Oversight Systems
Pindrop Security
Pramana
Quest Software
SAI Global
Secure Computing Corp (McAfee)
Skybox Security
Stonesoft
Threatmetrix
TrustStamp
VeriSign
Vonahi Security
WiKID Systems
Xtreme Security

## INFOSEC SOLUTIONS/SERVICES COMPANIES

Abacus Solutions
Adams Data Management
Axway Inc
Bastille - Security for the Internet of Radios
BeyondTrust
Bluefin
Capital Data Service Inc
Clear Skies Security
ControlScan
CoreGuard
Core Security
Curricula
Cybraics
Cybriant
Dell SecureWorks
Eclipse Networks, Inc.
Endgame Systems
EnterEdge Technology
Evident ID
Extreme Clarity Solutions
Forsythe Solutions Group
Gladiator Technology Services
Global Crypto
HPE
Intelligence One
Ionic Security Inc.
Ledgr
Liberty Technology Inc
MetricStream Inc
NCC Group
nuBridges Inc
Orasi Software Inc
Orion
PerformanceIT Inc
Perket Technologies
PurpleBox Security
Risk3Sixty
Safe Systems Inc
SA IT Services
Securolytics
Simeio
Telemetry Labs
TrustNet Inc
VC3
VMware
Zscaler

## EARLY INNOVATORS

The Georgia InfoSec and Cybersecurity market has many innovators. Here are three organizations that helped define the ecosystem.

**Internet Security Systems (ISS):** founded in 1994 by Chris Klaus as a student at Georgia Tech, ISS has been a mainstay in the cybersecurity technology market. ISS provides security solutions to thousands of the world's leading companies and governments, helping to proactively protect against Internet threats across networks, desktops and servers. ISS software, appliances and services monitor and manage network vulnerabilities and rapidly respond in advance of potential threats. ISS was sold to IBM in 2006 for $1.3 billion.

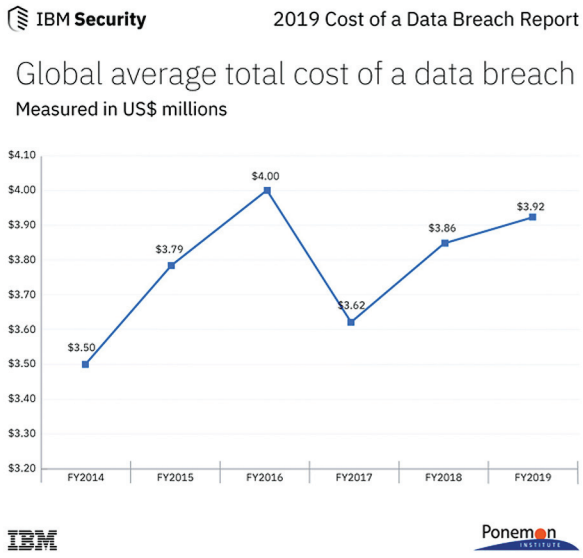
**Secureworks:** founded as a privately held company in 1998 by Michael Pearson and Joan Wilbanks. The company provides information security services, protecting its customers' computers, networks and information assets from malicious activity such as cybercrime. The company has approximately 4,400 customers across 61 countries, ranging from Fortune 100 companies to mid-sized businesses in a variety of industries. It became part of Dell in February 2011 and branched off to become a public organization in April 2016. It is still majority-owned by Dell.

**AirWatch:** founded in 2003 by John Marshall. AirWatch is a leading provider of enterprise-wide mobile device and WLAN management solutions to track, monitor and manage an enterprise's entire fleet of mobile devices. The company was acquired by VMware, Inc. in February 2014.

*Continued from page 3*

adoption curve:

- 84 percent of enterprises have a multi-cloud strategy including a mixture of public and private clouds
- 82 percent say they will increase spending on analytics and operations to improve responsiveness to security threats
- Less than 50 percent of organizations believe their security infrastructure facilitates compliance and regulatory enforcement




*The time it takes organizations to identify and contain a breach — what we call the data breach life cycle — is 279 days. The 2019 life cycle is 4.9 percent longer than the 266 day average in 2018. In addition, we found that the longer a breach's life cycle is, the greater the total cost. This is especially true in the case of malicious and criminal attacks, which take an average of 314 days to identify and contain. (2018 Ponemon Institute LLC for IBM)*

***Services (subscription and managed) will represent at least 50% of security software delivery by 2020. (2018 Gartner Group)***

### Skilled Professionals Needed - Now

Employment of information security analysts is projected to grow 32 percent from 2018 to 2028, according to the Bureau of Labor Statistics.

*Continued on page 7*

# BY THE NUMBERS

Information Security Industry
Georgia, 2018

TAG | Information Security

**Employment**[3]
6,687

**State Wide Est. Economic Impact**[2]
$2.6B

**Top 20 Companies Est. Revenue (GA)**[2]
$1.3B

**Venture Capital Deals**[3]
12

**Companies**[5]
77

**State Wide Est. Revenue**[2]
$1.4B

**Top 20 Companies Est. Revenue per Person(GA)**[2]
$207K

**Disclosed Venture Capital Raised**[3]
$818M

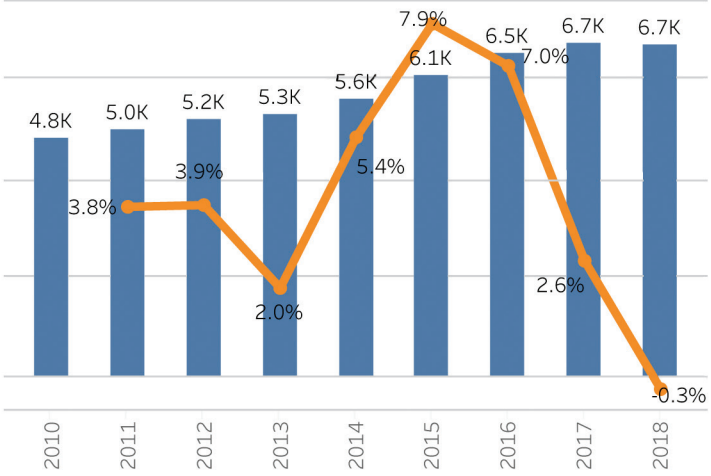
## INDUSTRY DEFINITION

There are 77 Information Security companies in Georgia according to the Technology Association of Georgia (TAG). TAG compiled a list of companies in the Information Security industry with operations in Georgia, and each figure reported here is a total for these identified companies' operations within the state.

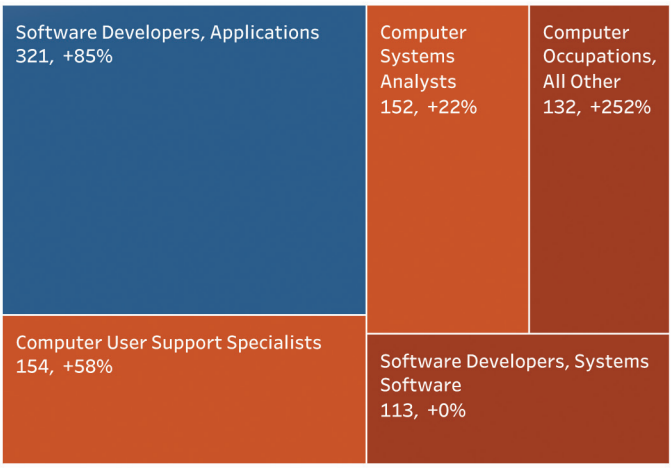
## INDUSTRY HIGHLIGHTS

There are nearly 6.7K jobs in the Information Security industry, which has grown from 4.8K in 2010. The total industry has a $2.6B economic impact to the State of Georgia and $1.4B in estimated statewide revenue. The 20 largest employers claim almost all of this revenue, at $1.3B. Over $800M in venture capital funds was raised in 2018 through 12 deals.

### Employment, 2010-2018
& Year-over Year Growth (%)[4]



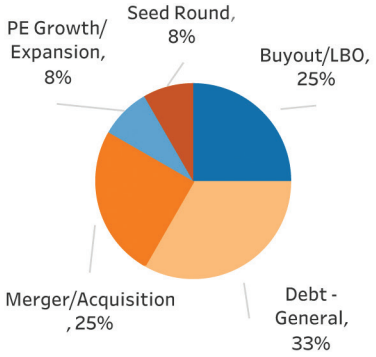

### Top 5 Technical Occupations
Number of Jobs; Growth since 2010 (%)[4]



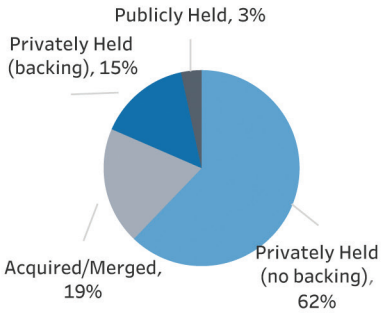

### Top 20 Employers
Alphabetical Order[1]

| | |
|---|---|
| Abacus Solutions | Lancope |
| Barracuda | Motorola Solutions |
| Blough Tech Inc | Numerex Solutions LLC |
| ControlScan | Orasi Software Inc |
| Dell SecureWorks | Oversight Systems |
| EMC Corp/RSA Security | PerformanceIT Inc |
| Gladiator Technology Services | Pindrop Security |
| IBM Internet Security Systems | Safe Systems Inc |
| Ionic Security Inc. | Secure Computing Corp |
| Ipswitch Inc | Simei |

### Venture Capital Deals by Type[3]




### Companies by Ownership Status[3]




Sources
[1]Quarterly Unemployment Insurance Match Data
[2]Center for Economic Development Research, Georgia Institute of Technology, IMPLAN Model of Georgia
[3]Advanced Technology Development Center, Georgia Institute of Technology, Pitchbook
[4]EMSI
[5]Technology Association of Georgia

Georgia Tech | Center for Economic Development Research

*Continued from page 5*

This is a much higher growth rate than the average for all occupations.

The Information Systems Audit and Control Association (ISACA), a non-profit information security advocacy group, predicts there will be a global shortage of two million cyber security professionals by 2019. Every year in the U.S., 40,000 jobs for information security analysts go unfilled, and employers are struggling to fill 200,000 other cybersecurity-related roles, according to cyber security data tool CyberSeek.

Privacy concerns are also becoming a key factor. According to Gartner, privacy concerns will drive at least 10 percent of market demand for security services through 2019 and will impact a variety of segments, such as identity and access management (IAM), identity governance and administration (IGA) and data loss prevention (DLP).

Gartner believes data privacy concerns will drive at least 10 percent of market demand for security services through 2019 and will impact a variety of segments. The analyst firm expects particularly high demand for

*Continued on page 10*


## COST OF DATA BREACHES

According to IBM, the impact of a data breach on an organization averages $3.86 million, though more serious "mega breaches" can cost hundreds of millions of dollars. The potential cost of an incident depends on several factors with the financial impact rising in line with the number of records stolen. On average, each record costs $148 and a breach of 1 million records costs $40 million while a breach of 50 million records costs $350 million. The research also found that the efficiency in identifying an incident and the speed of the response have a huge impact on a breach's overall cost. On average, it took companies 197 days to identify a data breach and 69 days to contain it.

# INFOSEC COMPANY CASE STUDY CONTROLSCAN® (ALPHARETTA, GA)

## The Challenge: Myriad Points of Vulnerability, Limited IT Resources

Like many independent grocery retailers, Chicago-based Fairplay Finer Foods started out with a single store and has added locations over its 40-plus years in business. And, since 1993, Fairplay has contracted with KCS Computer Technology, Inc., which established and now manages a corporate IT network across its chain of seven stores.

While Fairplay's business growth represents strong market traction, the increased sophistication introduces additional IT needs and information security risks. This issue presents a significant challenge for IT firms, because effectively identifying and mitigating every point of vulnerability (PoV)—especially in a chain store setting—requires the time and expertise of a security specialist.

Understanding the need for additional resources to properly address the security risks and compliance requirements chain stores face, Fairplay and KCS joined forces in 2014 to identify Alpharetta-based ControlScan as a suitable solution provider.

## The Solution: A Managed Security Services Partnership

ControlScan presented a simple pricing model for a Managed Security Services (MSS) partnership, whereby ControlScan serves as an extension of KCS to deliver cloud-based security technologies and related support services:

- Installing, configuring and monitoring a system of next-generation firewalls;
- Investigating, responding to, and reporting on security events;
- Providing utilization reports for insights into company resource usage;
- Implementing the latest security enhancements; and
- Lending expertise to reduce complexity and contain costs.

Along with its MSS proposal, ControlScan suggested that Fairplay undergo a PCI Gap Analysis to compare current security controls with those required by the Payment Card Industry Data Security Standard (PCI DSS). Any "gaps" ControlScan discovered would then be converted into a detailed set of recommendations and options for remediating gaps, reducing PCI scope and, ultimately, achieving PCI compliance.

## The Result: Unified Security and Compliance

Taking a unified approach to data security and compliance, ControlScan guided the Fairplay Finer Foods chain to a stronger security posture. ControlScan's Managed Security Services have allowed Fairplay to cost-effectively sustain a state of security that protects their business and the customers they serve. In addition, ControlScan's in-depth knowledge of how secure technologies and processes work together to meet PCI DSS requirements reduces time and costs associated with maintaining continuous compliance.

More specifically, the managed security partnership with ControlScan brings Fairplay these benefits:

- No full-time security employee overhead, yet easy access to an expert team of professionals possessing security-specific certifications such as CISSP, CISM, Security+, ITIL v4, QSA, ASV, etc.;
- Reduced security infrastructure management costs through streamlined design and hardware life cycle maximization; and
- Round-the-clock security vigilance so that KCS can remain dedicated to overall IT performance.

## CONSUMER-FRIENDLY CCPA REQUIRES BUSINESSES TO PAY MUCH CLOSER ATTENTION TO USER DATA

The landmark consumer privacy law California Consumer Privacy Act (CCPA) is set to go into effect January 1, 2020. It allows any California consumer to demand to see all the information a company has saved on them, as well as a full list of all the third parties that data is shared with. In addition, the California law allows consumers to sue companies if the privacy guidelines are violated, even if there is no breach.

All companies that serve California residents and have at least $25 million in annual revenue must comply with the law. In addition, companies of any size that have personal data on at least 50,000 people or that collect more than half of their revenues from the sale of personal data, also fall under the law. Companies don't have to be based in California or have a physical presence there to fall under the law. They don't even have to be based in the United States. Companies have 30 days to comply with the law once regulators notify them of a violation. If the issue isn't resolved, there's a fine of up to $7,500 per record.

Companies must allow consumers to choose not to have their data shared with third parties. That means that companies will now have to be able to separate the data they collect according to the users' privacy choices. There's also another potential financial risk. The bill provides for an individual's right to sue, for the first time and it allows class action lawsuits for damages.

## EU GETS SERIOUS ABOUT PERSONAL DATA

The General Data Protection Regulation (GDPR) focuses on giving European Union citizens more control over the use of their data on the web and includes new rules on how organizations should handle that data.

The GDPR went into effect on May 25, 2018. Although the regulation is based in Europe, it is more far-reaching than it seems at first glance. If your business has any connection to Europe, whether through customers or partners (even just one!), you should be aware of what the law requires.  GDPR states that any information "specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person" are under protection.

The updated policies must include information about what data is collected, why it's being collected, how long it will be stored, as well as how it will be used and who will have access to the data. This needs to be stated clearly on the website in a noticeable place. GDPR compliance requires active consent — not passive methods, like a pre-checked box. The GDPR will have little tolerance for dark UX practices that trick people into agreeing to or signing up for things, or poor blog design that hides pertinent information.

Companies should contact legal and other professionals for advice on CCPA and GDPR complience.

*Continued from page 7*

people with skills in privacy-related security areas such as identity and access management (IAM), identity governance and administration (IGA) and data loss prevention (DLP).

***Financial services dominates spending within the 11% to 20% and 21% to 30% ranges, with 28% of respondents selecting each. Meanwhile, public sector and healthcare respondents led the group spending less than 10%. (2018 Forrester Research)***

"Security leaders are striving to help their organizations securely use technology platforms to become more competitive and drive growth for the business," said Siddharth Deshpande, research director at Gartner. "Persisting skills shortages and regulatory changes like the EU's Global Data Protection Regulation (GDPR) are driving continued growth in the security services market."

Indeed's 2019 research shows the metro areas with the most cybersecurity job postings, by ranking, are:

1. Washington, DC
2. New York, NY
3. Dallas-Fort Worth, TX
4. Baltimore, MD
5. Chicago, IL
6. **Atlanta, GA**

## Georgia Fosters Strong Market Dynamics

As one of America's elite cybersecurity hubs, Georgia has fostered a healthy infrastructure to support the growth of InfoSec and cybersecurity technology companies. The InfoSec and cybersecurity infrastructure is supported by a very well-connected technology community and educational system.

An excellent example of this is The U.S. Cyber Command located in Augusta GA.

## GEORGIA CYBER CENTER

The Georgia Cyber Center, located at Augusta University in Augusta, GA, is a unique public/private collaboration among academia, state, federal and local government, law enforcement, the U.S. Army and the private sector. With two adjacent buildings totaling 332,000 square feet, the Georgia Cyber Center, located on the Nathan Deal Campus for Innovation, is designed to meet the growing need for cybersecurity talent in Georgia, the nation and across the globe.

The Georgia Cyber Center, a first of its kind collaborative cybersecurity center located in Augusta, Georgia, opened its doors on Tuesday, July 10, 2018, with a grand opening ceremony. The $100 million Cyber Center is the single largest investment in a cybersecurity facility by a state government to date, strengthening the state of Georgia's position as a national leader in cybersecurity.

The Georgia Cyber Center is the single largest investment in a cybersecurity facility by a state government.


## DEPARTMENT OF DEFENSE DEFINES SECURITY FRAMEWORK

Government organizations are just as likely to suffer data breaches as any other business and are increasingly and specifically targeted. To improve data security, the U.S. Department of Defense (DoD) will be implementing a security framework called the Cybersecurity Maturity Model Certification (CMMC) for all third-party vendors. CMMC is a supply chain risk management approach to reduce the risk resulting from cyberthreats. Soon certifiers will have the tools to conduct audits and collect metrics and risk management information for the entire supply chain. Please contact Heather Maxfield, TAG's Vice President, Government Affairs & Statewide Economic Development for more information.

The Cyber Command is part of the U.S military and charged with monitoring and managing the existing cyberspace operations and cybersecurity of military and government IT and Internet operations. U.S. Cyber Command was initiated in 2009 to create a separate military wing for cyberspace operations and security.

*2019 will be a year of unprecedented cyberthreats to companies and individuals. And it will be a year when governments and companies turn to Zero Trust.*

Cybersecurity and defense depend on recruiting, training and retaining quality talent, and Georgia is committed to providing InfoSec companies access to a pipeline of qualified talent.

Educational partners training the next wave of practitioners are critical for the continued advancement of the InfoSec and cybersecurity ecosystem.

- Georgia is in the top 10 states with Centers of Academic Excellence in Cyber Defense (CAE-CD) across eight of the state's universities, designated by the NSA and the Department of Homeland Security.
- Georgia Tech's Institute for Information Security & Privacy combines the expertise of 200 researchers and nine labs with the Georgia Tech Research Institute (GTRI) to collaborate on all cybersecurity efforts – connecting academia, industry and government.
- The Augusta Cyber Institute at Augusta University is geographically situated at the center of key federal and infrastructure assets, including the NSA, Army Cyber Command, the Georgia Cyber Center, the Army Cyber Institute, and the Cyber Center of Excellence.

- Georgia created the nation's first FinTech Academy, combining the University System of Georgia's 26 public institutions with 120+ companies to train a robust workforce of fintech and cyber warriors.

***With stolen medical records being sold on the black market for up to 60 times that of stolen credit card data, it's no wonder that healthcare organizations are consistently ranked No.1 or No.2 in lists of industries with the highest amount of data breaches. (2019 Secureworks)***

Georgia is home to 8 nationally ranked cyber institutes with CAE-R (Cyber Research) CAE-CD (Cyber Defense) designations, numerous cyber research centers, and ranks in the top 10 states for most centers of academic excellence.

- Augusta University – CAE-CD
- Columbus State University – CAE-CD
- Georgia Institute of Technology – CAE-R (research)
- Georgia Southern University (Armstrong State University) – CAE-CD
- Kennesaw State University – CAE-CD
- Middle Georgia State University – CAE-CD
- University of Georgia – CAE-R (research)
- University of North Georgia – CAE-CD

## KEY INFOSEC/CYBERSECURITY TRENDS

### Effective Solutions for Hybrid Cloud Security will be Priority


Organizations are embracing a hybrid IT infrastructure of cloud, third-party services and microservices, which provides the necessary flexibility and scalability. With resources spread across on premise, private and public clouds, organizations do not have centralized control and visibility, leaving many security gaps. As hybrid environments can strain traditional solutions designed for more static environments, businesses will have to ensure that their security is not left behind.

### Businesses and Cybercriminals Alike will Leverage AI, ML

Artificial Intelligence (AI) is taking center-stage in cybersecurity and consists of Machine Learning (ML), which has the potential to identify and respond to threats as they occur. As AI and ML can help turn volumes of data into actionable insights, they can tangibly improve organizations' cybersecurity efforts.

### Automation will Create Efficiencies

Robotic Process Automation (RPA) in particular, automation eliminates the risk of human errors from tedious manual work and allows them to focus on more proactive tasks will increase in the area of cybersecurity, including Incident detention, analysis and response. The scope of automation will also expand in 2019, where robots and machines will automatically remediate some of the security issues, which were manual focused.

### IoT Attacks will Increase in Number

The risks of cyberattack increase proportionately to the growth of Internet of Things (IoT) implementations, Driverless cars, smart cities, smart homes, smart watches and virtual assistants are all part of the Internet of Things (IoT) revolution and are gaining popularity. IoT implementations are often not secure end-to-end (from field level devices and gateways to the cloud-based applications and APIs). Malicious hackers will find the gaps unless organizations are diligent about shoring them up. In addition, regulatory security standards are needed that require device manufacturers and software providers to comply.

### Increased Attacks on Small Businesses and Individuals

Attacks will be spread out and a greater number of small businesses and even individuals will come to the attention of cybercriminals. Large organizations have already done considerable work to protect themselves from attacks. It is easier to target small and mid-size companies as they may not have adequate security measures and resources in place to protect themselves. Small companies must re-assess their security posture and ensure adequate

measures and controls are implemented to safeguard against today's cyberattacks.

**Data Privacy Laws Go Big**

The dynamic nature of cybersecurity typically outruns regulations, but there will be a paradigm shift in the ways companies will use and manage data in 2019. In the light of high-profile data breach incidents, customers are worried and are demanding better protection measures. Governments and regulatory bodies are also concerned. This coupled with the implementation of the General Data Protection Regulation (GDPR) in the EU and the enactment of the California Consumer Privacy Act (CCPA) in the US, among others, is forcing companies to look at privacy issues more seriously and prepare for more data privacy regulations in 2020 and beyond. Such laws are making companies move from a reactive approach to a proactive approach to security. As privacy-related compliance goes up, the onus will be on respective organizations to implement robust security measures and practices.

Source: Security Magazine

# ABOUT US

## TAG Information Security

The TAG Information Security society's mission is to provide a leadership forum focused on education and collaborative sharing of today's information security, privacy, risk management and compliance related issues. Keeping you informed, allowing community collaboration and facilitating an open exchange are our primary goals. The society is positioned well for business and technology professionals interested or actively working in the field of information security, privacy, risk or compliance. If you have an interest in learning and exchanging information on how and why integrating information security in your business then you should attend.

Key Strategies:

- Develop a sustainable community for leaders within the Security, Risk and Compliance Industry
- Provide educational and networking opportunities for security leaders
- Provide visibility to emerging trends, technology and enterprises that excel in Information Security, Privacy, Risk Management and Compliance

## Technology Association of Georgia

TAG is the leading technology industry association in the state, serving more than 30,000 members through regional chapters in Metro Atlanta, Athens, Augusta, Columbus, Macon/Middle Georgia, and Savannah. TAG's mission is to educate, promote, influence and unite Georgia's technology community to foster an innovative and connected marketplace to fuel the innovation economy.

The association provides networking and educational programs; celebrates Georgia's technology leaders and companies; and advocates for legislative action that enhances the state's economic climate for technology. TAG hosts over 200 events each year and serves as an umbrella organization for 26 professional societies. Additionally, the TAG Education Collaborative (TAG-Ed) focuses on helping science, technology, engineering and math (STEM) education initiatives thrive.

For more information visit the TAG website at www.tagonline.org or TAG's community website at www.hubga.com. To learn about the TAG-Ed Collaborative visit http://www.tagedonline.org/.

# SPONSORS

## GOOGLE

Google's mission is to organize the world's information and make it universally accessible and useful. Their key commitments include the following: protecting users, expanding opportunity, including all voices, responding to crises, and advancing sustainability. Some of their key services include YouTube, Google Search, Google Chrome, and Google Maps. They also have products such as the Google Pixel and Google Home.

## SAGE

Sage Business Cloud is changing how businesses compete and grow, by delivering faster, simpler and flexible financial, supply chain and production management, at a fraction of the cost and complexity of typical enterprise ERP systems. The industries that are covered as of now are distribution, process and discrete manufacturing, food and beverage, chemicals, and services.

## SCIENTIFIC GAMES

With global Lottery group headquarters located in metro Atlanta, Scientific Games is a world leader in entertainment offering dynamic games, systems and services for casinos, lotteries, online gaming and sports betting. Since 1973, the company is a trusted supplier of games, technology and services to regulated gaming organizations and lotteries around the world, including the Georgia Lottery and nearly every North American lottery. Scientific Games offers the gaming industry's broadest and most integrated portfolio of game content, advanced systems, cutting-edge platforms and professional services. Committed to responsible gaming, Scientific Games delivers what customers and players value most: security, engaging entertainment content, operating efficiencies and innovative technology. For more information, please visit scientificgames.com.

## NCC GROUP

NCC Group (https://www.nccgroup.trust) is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape. With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate & respond to the risks they face. NCC Group is passionate about making the Internet safer and revolutionizing the way in which organizations think about cyber security.