NETWORK INTELLIGENCE
Global cybersecurity provider

ANNUAL CYBERSECURITY TRENDS AND PREDICTIONS

2019

Foreword

As we start 2019, we can clearly see that IoT & Digital Transformation will play a key role in our day to day lives. Typically, these technologies are meant to help & assist us, but threat actors of the cyber world, exploit these same technologies for their own good.

There is of course no way we can turn back this inevitable technology revolution.

And while there is no single silver bullet in security, and we do know that investments in security technologies will continue to grow, the real impact is seen when there's cultural shift within an organization in terms of their attitude towards data protection. And this cultural shift is most effective when it begins with the Board and senior management moving in the right direction.

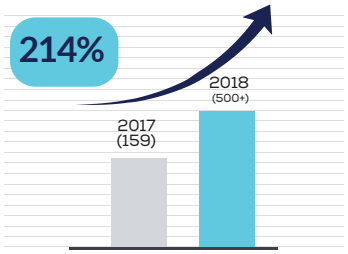
For us as a company, we asked our Practice Leads to put together the insights they learnt from the ground in each of their practice areas and what they foresee as some of the key trends for 2019.

From my end as the Global Business Head, I am happy to share some of the key business highlights of the year for us:

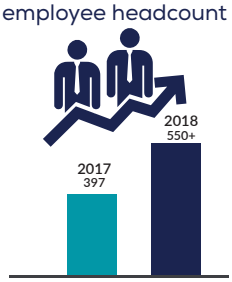
Y-O-Y Growth in Revenue.

48%

Y-O-Y growth in employee certifications

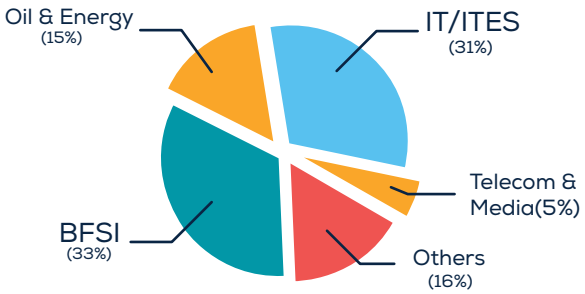


Y-O-Y growth in employee headcount

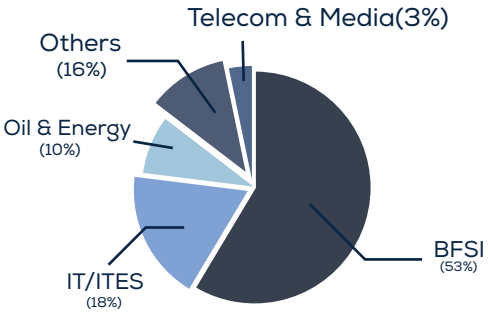


38% increase in the headcount

Industry-wise Customer Breakup



Industry-wise Revenue Breakup



I do hope that these insights will prove useful for your cybersecurity initiatives.

Altaf Halde
Global Business Head

Research & Innovation

2018 had been a tumultuous year for the cybersecurity industry.

The year started with critical vulnerabilities like Meltdown and Spectre, where we were informed of the massive breaches via the SWIFT network in Malaysia and India. 2018 also saw GDPR regulations coming into force with many companies struggling to inform users of the change in data-collection and maintenance policies. In terms of cybersecurity innovations, the year saw start-ups building solutions in the machine learning space and Make-in-India movement boosting the development of cybersecurity products in the country.

Cloud has not only been adopted by enterprises but also by cybersecurity companies for service delivery. With data volume for security monitoring increasing by the day, cloud provides an extensible platform for both customers and services providers to scale up their operations smoothly. It is expected that rather than investing in on-premise SIEM technologies, companies would prefer SIEM-as-a-service due to cost effectiveness.

Security Incident response processes were a key area of CISOs' focus in 2018. KPIs of Blue Teams were defined taking mean-time-to-detect (MTTD) and mean-time-to-response (MTTR) into consideration. These two metrics are likely to drive IR process improvement in 2019 as well. Automation and orchestration will help measure and improve the metrics for security teams. However, coordination and support from IT teams will play a major factor in the success of such initiatives.

Total number of threat hunting use cases developed

What does 2019 hold for the market?

An interesting trend that was observed over the past year was the huge investments that enterprises made in new detection and visibility capabilities as compared to prevention technologies. Network visibility weighed higher for security teams when evaluating cyber-security solutions. We foresee more traction for service and solution providers who can enhance their Blue Team's view into their infrastructure. Visibility in terms of endpoints, east-west traffic, remote locations, cloud services, third party vendors etc. will be the next focus area of organizations.

Organizations now seem to have been convinced on the idea of using machine learning based products for better threat detection as attackers are continuously building TTPs (tools, techniques and procedures) which function under the radar and live-off-the-land. While the use of machine learning techniques by Blue Teams is believed to grow manifold and mature in 2019, it is wise to also expect the attackers to use the same technology to build adversarial machine learning capabilities.

2018 saw rapid adoption of cloud services across industries. Although BFSI industries are still playing it safe due to strict regulatory norms, other industries have embraced the move towards cloud computing, both for internal consumption and service delivery. Setting up of local data centers by leading cloud service providers (CSP) have also eased the customers' concerns. With cloud infrastructure being added into the IT-infra mix, enterprises have also started the integration of logs from cloud apps and services into their existing SIEM solutions. It is believed that more companies will push towards cloud migration in the coming year.

Government regulations will pay an important role as well due to the requirements of localization of cloud data collection and hosting. Security service providers should expect customers wanting their data stored only in local cloud data centers to comply with government regulations (GDPR, Data Protection bill etc.). This, however, will lead to added costs for customers.

2019 will surely be a heck of a ride!

Contributed By Wasim Halani, Head – Research & Innovation

Security Assessment

The rapid adoption of Digital Transformation initiatives we saw a number of security assessment projects that involved cloud computing, APIs, DevOps and new technologies. We also saw more organizations maturing in embedding security into their software development lifecycles – i.e. shifting security "left" – by involving security teams from the design stage onwards.

Cloud: The old objections to cloud computing started to fall off, and CISOs were often asked to facilitate cloud adoption by business units and CIOs. Even with Banks, we saw some major systems being moved to the cloud, such as CRM and HRMS applications or migrating to Office 365 and G Suite. This obviously required us to come in and assess cloud security setups and ensure that in many of these hybrid cloud situations, security at the network architecture level, application level, identity federation levels were properly addressed. In fact, we ensured that our product Firesec™ had capability added to assess AWS and Azure network security configurations.

Adversary Simulations: Our red team assessment practice improved dramatically, where we started using FUD – Fully Undetectable Malware. In fact, one of our leading pen-testers wrote a very popular 3-part blog series on writing such malware to evade detection by most security technologies.

Automation: Not only did we see automation disrupting business models for our clients, but at our end also we significantly invested in automation tools for our assessment practice by partnering with Qualys (for vulnerability management, configuration audit, web application security assessments), AppKnox (for mobile application assessment), Checkmarx (source code review), etc.

DevSecOps: In line with the adoption of DevOps, we partnered with the above companies to help our clients implement DevSecOps within their development processes.

5 uncommon vulnerabilities found this year

- Attacks against XML Parser – XXE, Billion Laugh Attacks
- Session Takeover via Heartbleed
- Session Puzzling
- SQL Injection via CSRF token Bypass
- Invisible backdoor admin account

IoT and ICS Security: Finally, one of the most interesting areas in which we were able to rapidly build capability was in security testing of IoT (Internet of Things) and Critical Infrastructure. We carried out some of the largest ICS Security assessment projects in India and the Middle East. And our practice in this area has kicked into high gear already with the start of the new year.

Cloud Security Projects

150% rise in Cloud Security projects

Red Team Assessment Projects

133% increase in
Red Team Assessment projects

What does 2019 hold for the market?

The year 2019 will see major trends in the following domains:

Automation:

We will continue to invest in automation and choosing the right tools to help deliver projects faster, with more comprehensive coverage, and reduced false positives.

Adversary simulation:

We are evolving our red team assessment service into "adversary simulation" Adversary simulation extends the red team assessment exercise to involve the blue team and see how the organization will be able to respond to a real attack.

IoT level attacks:

The rapid adoption of IoT and Industrial IoT does not seem to be keeping cybersecurity controls at the right priority. We already saw the Mirae botnet exploit IoT devices to launch one of the largest Denial of Service attacks the world has seen. We have also launched an IoT security training course as well.

Cloud-service demand and security flaws:

We also perceive that breaches involving cloud computing will only increase, as cloud adoption is now inevitable. And almost every new-age startup is a born-in-the-cloud company.

Partnerships with security firms:

Financial organizations will team up with security firms like Network Intelligence to implement new technologies along with adopting new cultures such as DevSecOps.

Others:

Technologies like the 5G will introduce new threats along with new techniques a rise in advanced ransomware. Awareness towards cyberattacks will require training on new technologies, frauds, attack vectors, secure coding and much more.

Contributed By Shrikant Antre, Practice Lead - Assessment

Managed Security Services

As my colleagues noted in the earlier sections, digital transformation, rapid technology adoption has disrupted traditional ways of doing business across the world. This has naturally led to cyber-security challenges and increased regulatory oversight.

Shortage of cybersecurity professionals with strong expertise & the need to get effective security delivered without heavy capex costs have been the key drivers in the growth of the MSSP business around the world and is expected to grow at an even faster pace in 2019.

Large Organizations have been seeking more advanced Managed Security Services to reduce the risks & enhance their security threat management. They look for an advanced set of services like **Threat Hunting, Threat Response, Threat Intelligence** etc. On the other hand, small businesses are still looking for standard service offerings like Log Monitoring, Infrastructure Assessment & Management, Device Management etc. from MSS providers.

It has been observed that there is a huge demand for **Managed Detection & Response** service and it is believed that Indian companies will start to adopt it in the coming years. They also seem to have realised that only threat detection won't suffice instead a fast response to the threats & their remediation will be required to stand a chance against the ever-evolving cyber-attacks. All of this saw a massive uptick in our MSSP business as we partnered with IBM and brought the QRadar platform for our customers.

Growth in MSSP business

What does 2019 hold for the market?

Large organizations can afford an in-house team to manage security, and they might have a resiliency plan, but it is SMB market that lacks the resources to build 24x7 Threat Detection & Response capabilities. These organizations are the best fit for the MSSP market.

Another trend that has been observed in the market is the growing demand for automation. The cybersecurity industry is still too human-dependent. No matter how many stacks of technologies an organization has, their efficiency of is dependent on people managing them and with a shortage of skilled resources in the market, organizations have understood the importance of building automation in technology & processes which can reduce the dependency on human beings. In fact, large companies in India; especially from the banking sector have started their journey of upgrading their respective security teams with Next-Generation tools and technologies capable of identifying threats at a much earlier stage in the Cyber Kill Chain and have quicker response capabilities to minimize the threat impact.
Apart from this, owing to the cost-saving, agile & flexible offerings of cloud environment, a lot of organizations are moving towards cloud. We have adapted our MSSP services to be completely cloud-friendly and in fact our BlueScope™ platform is built and delivered via the cloud.

In this year we expect to see more organizations focusing on managing threats, adopting a risk-based approach to security spending and continuing to ramp up their efforts to improve their security posture with the help of MSSPs.

Contributed By Aniket Govilkar, Practice Lead - MSSP

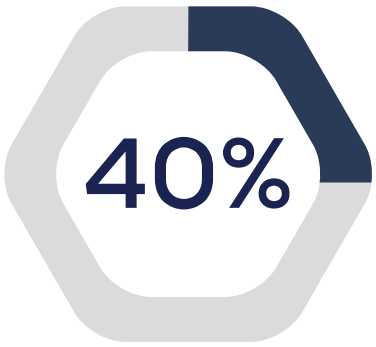
Payments Security

As per Verizon's 2018 payment security report, it is scary to see a drop in the organizations getting fully PCI DSS compliant for the very first time in the last five years. What's even scarier is, the fact that PCI DSS certified organizations are failing to maintain PCI DSS compliance throughout the year and it keeps getting worse with each year passing. This has, in a way, resulted in a lot of breaches in 2018 which also included some PCI DSS certified organizations.

While, many organizations still look at PCI DSS Compliance as the end goal for security, it should primarily be treated as a measurement metric for an organization to record, maintain and improve its efforts towards protecting the cardholder data. With breaches becoming everyday news; organizations must remain cautious, vigilant and make payment security as part of their business as a crucial activity. While, 2018 saw a lot of new evolved technologies in the payment space with an aim to ease the payment process for consumers; a quick fact-check on the security aspect of these technologies has still been a key concern. That being said, 2018 has seen good shift from **stripe cards to chips cards** but there is still a long way to go.

Some of the prominent breaches that happened in 2018 taught one key lesson and that is, while breaches are scary, what is more alarming is the damage caused due to the failure of an organization's approach towards accepting and identifying the breach at an early stage and their lack of ability to control the incident. 2019 may compel organizations to have a robust incident management team (not just a policy document but a practical approach plan); perform periodic red team assessment, proper forensics retainers, and most importantly include payment security leads in board room meetings.

PCI DSS Projects



Increase in PCI DSS Projects

What does 2019 hold for the market?

Data leakage through APIs and Data Scraping: Most businesses are widely using APIs and exposing their data to scraping attacks. Many startups are collecting terabytes of data per day using data scraping and their entire business models depend on this. One of the major challenges in 2019 will be to protect APIs and control the data shared through these APIs.

Cloud and DevOps: How do we ensure PCI DSS compliance in a DevOps environment? This is a question our consultants face and answer so often nowadays that we have developed a DevSecOps go-to document. If an insurance company is implementing a chatbot, how does Microsoft Cortana ensure that PCI DSS compliance is taken care of if a customer shares their card number during the chat? These challenges will continue to keep our QSAs on their toes and we look forward to helping companies not just comply with PCI DSS, but implement real security to protect cardholder data.

IDaaS (Identity Management-as-a-Service): As organizations migrate to the cloud, so do identity services like active directory & privileged identity management. Since, IDaaS is currently used to provide authentication services to cloud infrastructure, this could be a single point of failure and proper controls must be implemented to protect them from cybercriminals.

Blockchain for securing payments: The idea of a secured storage and transmission of data through a decentralized database is the most attractive feature of blockchain technology. Originally used for cryptocurrency transactions, the system is believed to be transparent, incorruptible and meant to provide unaltered information. Like any technology, blockchain will be vulnerable to compromise. Potential vulnerabilities include weak encryption, hashing and key management; poorly written programs; incorrect permissions; and inadequate business rules. Security teams will have to play a vital role in various phases of blockchain application development.

Customers information security awareness: As the companies get affected by card data breaches, it forces them to become more aware of the importance of payment security. It has in turn increased their expectations. Now, they would not only be looking for security compliance but also assurance on data safeguard and an effective mitigation of the risks.

Our PCI DSS practice in 2018 doubled when compared to the business we did in 2017. In 2019, we expect to grow it nearly three times as we have acquired licenses for almost the entire globe and expanded our QSA team size as well.

Contributed By Deep Chanda, Business Head – Payments Security
& Manish Chaudhari Practice Lead - PCI DSS

Governance, Risk Management & Compliance (GRC)

In 2018, our GRC team was occupied in addressing compliance requirements that saw a surge due to the GDPR deadline lapsing in May 2018, increasing digitization leading to higher adoption of PCI DSS, and overall ISO 27001 becoming the global benchmark for cybersecurity frameworks.

We also started using the NIST Cybersecurity Framework and NERC-CIP for critical infrastructure security assessments. Various country-specific cybersecurity regulations also came into the picture.

In India, there was a dramatic increase in automation in the financial industry and a surge in cash-less transactions post the digitization initiatives led by the government and supposed by the regulators such as RBI, IRDAI, UIDAI, SEBI, and NPCI. The most interesting trend we saw come out explicitly in India was to enforce data localization on financial service providers. This prompted cloud service providers to expedite setting up India-located data centers.

Similarly, in the Middle East, increased awareness and major incidents made the regulators more active and they mandated that these cybersecurity requirements be audited on a yearly basis.

BCMS Projects

Increase in BCMS Projects

GDPR Projects

SWIFT has released their Customer Security Program (CSP) 2019 guideline and made it mandatory for all their customers to conduct an audit on a yearly basis. Adding to CSP requirements, RBI also released a circular post the Punjab National Bank – Nirav Modi fraud to have an integration of the bank's core banking application with the SWIFT system.

Network Intelligence got the opportunity to help set up India's 3rd SWIFT Service Bureau, which was a milestone for our GRC team.

Business Continuity (BCMS) consulting requirements were found to be on the rise in India & the Middle East with the company acquiring some good customers. There was a huge surge in the requirement for Third party audits for banks, Data Classification through DLP and IAM solutioning, GDPR compliance, Information Assurance in both India & Middle East region.

What does 2019 hold for the GRC market?

Compliance audits, third party vendor audits and ISO 27001 / ISMS consulting would remain the major drivers for our GRC practice in the coming year. We foresee increased adoption of NIST/NERC-CIP standards for Industrial Control Systems. We will continue to invest in getting our GRC team trained and certified across multiple standards and frameworks.

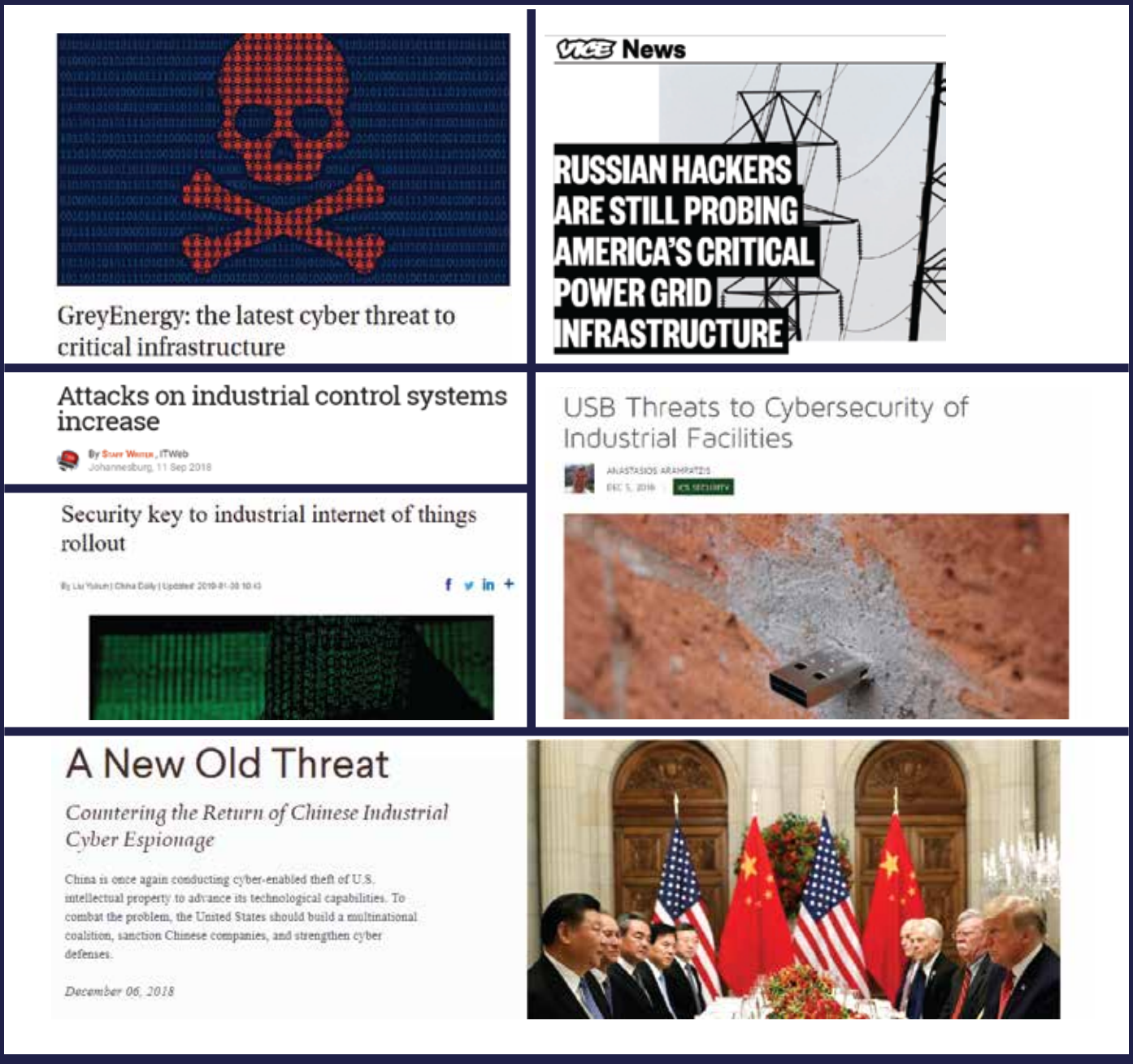
As a result of increased automation across industries, there will be a huge demand for cloud computing and ensuring compliance while moving to the cloud. Software-as-service (SaaS) is believed to grow at a rate of 18%, Platform-as-a-service (PaaS) may grow by 32% & Infrastructure-as- a-service by 12%. Almost all mid-sized organizations and start-ups have adopted cloud computing. Also, post GDPR, cloud security has become more stringent for organizations catering to EU customers.

Contributed By Ashutosh Mahashabde, Practice Lead - GRC

Industrial Cybersecurity (ICS)

Convergence of Information Technology and Operational Technology is expected to drive the overall growth of the Industrial Control Systems (ICS) cyber security market in 2019. The ICS cybersecurity market growth is driven by various factors, including huge investments by organizations in Industry 4.0/Industrial Internet of Things (IIoT), convergence of Information Technology (IT) and Operational Technology (OT), and rise in the number of cyber threats on the critical infrastructure. However, growing concerns about power outage, due to frequent security updates, and legacy ICS being more prone to cyber-attacks may hinder the growth of the market.

Some recent Industrial cyberattacks:



What does 2019 hold for the market?

The global industrial cybersecurity market is predicted to log a 9.2% CAGR during the forecast period 2018-2026 to reach a valuation of US$29.97 Bn by the end of 2026. In 2017, the global industrial cybersecurity market bagged a US$13.75 bn .

Effectively integrating security into an ICS requires defining and executing a comprehensive program that addresses all aspects of security, ranging from identifying objectives to day-to-day operation and ongoing auditing for compliance and improvement. The strategy for developing a security program, including the following:

- Obtain senior management buy-in
- Build and train a cross-functional team
- Define charter and scope
- Define specific ICS policies and procedures
- Define and inventory ICS assets
- Perform a risk and vulnerability assessment
- Define the mitigation controls
- Provide training and raise security awareness for ICS staff

Network Intelligence has developed an end-to-end approach to cyber, information, and operational security that establishes the trust and visibility required for the Industrial Internet. Our advisory and consulting approach ensures that both old and new OT infrastructure is protected against a variety of evolving threats, while also securing IT infrastructure and applications. Complete visibility and continuous monitoring ensure that the environment remains secure even as it grows in scope and scale.

As the Business Head for ICS Security – my vision is to establish strong practice delivery processes, partner with the right technology companies, and listen closely to client challenges as we assess their gaps and design security solutions and remediation strategies for them.

Contributed By Viral Trivedi, Business Head – ICS

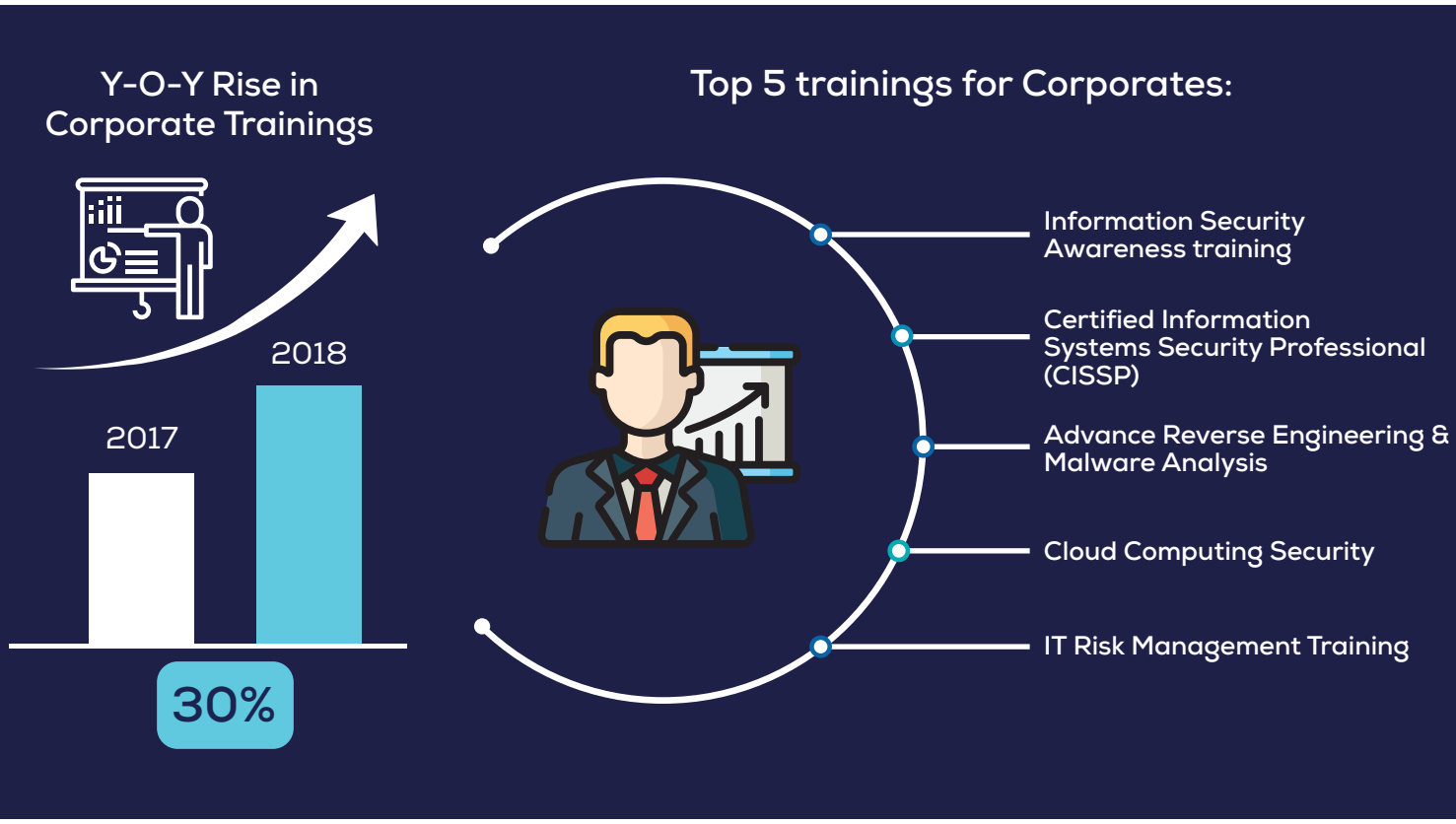
Transparency Market Research (https://www.transparencymarketresearch.com/industrial-cyber-security-market.html)

Cybersecurity Trainings

In 2008, we envisaged that going forward the demand for cybersecurity professionals is going to be the biggest challenge in the industry. Supply will not be able to keep pace with the demand. This set the ground for setting up the Institute of Information Security (IIS) now called Cyber Excellence Academy Pvt Ltd. (CAPL). Today we train more than 400 students each year, who in turn join various organizations in the cybersecurity domain.

While the demand for cybersecurity courses from the student community has seen growth, we have seen similar growth in the Corporate Training business as well. Our Security Awareness courses have seen a big jump among corporates and the important point is that our customers repeat these courses more than twice a year. This shows that organizations have now accepted that investing in technologies is not enough and that it has to be coupled with the spread of cybersecurity awareness at all levels in an organization and that too at regular intervals.

The demand for specialized courses has also seen a jump specifically in the technical courses related to Digital Forensics, Reverse Malware Engineering to name a few.



What does 2019 hold for the market?

With instances of targeted attacks increasing, we foresee the need of detecting threats and responding to them will drive the demand for Threat Hunting professionals, followed by security analytics using Big Data, Machine Learning. The Compliance market is something that will continue to be very much in demand including courses related to Data Privacy, PCI DSS, ISO 27001. While we see a shift in the market happening from a typical SOC (Security Operations Centre) to a Next GEN – CyberSOC, the requirement for specialized courses on Incident Response, SOC Management will be a trend in 2019

Contributed By Karishma Mookhey Co-Founder & Director – CAPL

Conclusion

In 2001, when I founded the company, I remember walking into the office of the Manager – Internet Banking of one of the large banks in the country and proposing to do a pen-test for their websites. His response was, we don't need to do this as we already have anti-virus. This response remained pretty much the same for a decade or so since then with anti-virus being replaced by firewalls and then by some other technology. But the past few years haven't been the same at all! Cybersecurity today is a board room agenda and business is growing at a pace that we sometimes find difficult to keep up with.

In fact, 2018 was one of the most remarkable years for us as a company. We strengthened our senior management team, raised a Series-A round of funding from Helix Investments, got our first product Firesec™ to market and made significant developments in BlueScope™ - our big data powered security analytics platform. We hired our US Head of Operations, Viral, who also leads our ICS Security Practice and grew our MSSP business dramatically. In fact, we won the contract to run the SOC for one of the largest banks in the country for a 3-year period.

Predicting what will happen in 2019 is an exercise fraught with the possibility of being terribly wrong. But I can definitely state areas in which we intend to focus in 2019 and the years beyond.

I believe the future of cybersecurity is in services. And services that are powered by automation will be the key differentiator of the future. That automation may come from our in-house efforts or it may come from the right technology partnerships. We will continue to invest significantly in developing BlueScope™ and Firesec™ and building automation via scripts on the MSSP front. We will also continue to keep a laser-sharp focus on learning and development of our teams. Be it IoT, ICS Security, Cloud Security, DevOps, GDPR, NIST – we want our teams to be sharp and on the cutting edge of technology developments and their security implications.

One of the hot topics in cybersecurity is the use of machine learning. In my view, there are certain areas in which ML has delivered exceedingly well – spam for example. In terms of detecting user and network behavior anomalies, we are beginning to see better results. However, in other areas, there is probably more hype than actual delivery on the ground. Yet, ML is the best hope we have of being able to process the massive amounts of data coming into our security infrastructure. And we are working on building better ML capabilities within both of our products.

Finally, I strongly believe that BlueScope, Firesec, our partnerships with IBM, Qualys and other technology partners will enable us to deliver tremendous value as a MSSP. Our constant focus on enhancing our capabilities on Threat Hunting, Red Team Assessments, and ICS Security will help us in providing cutting edge services to more mature clients.

We enter 2019 with a sense of higher expectations on ourselves and excited about growing our business in scale and depth.

K. K. Mookhey, Founder & CEO

Our Service Offerings

Assessment

- Web and Mobile Applications
- Code Review
- Network Architecture
- Infrastructure Vulnerability
- IoT, Blockchain, Cloud Security
- Red Team Assessments
- Bug Bounty Programs
- Critical Infrastructure (ICS)
- Telecom Infrastructure
- ERP

GRC

- Compliance Frameworks - NIST, GDPR, ISO 27001, ISO 22301, PCI DSS, HIPAA, SSAE18
- Policies & Procedures
- Security Awareness
- Risk Management
- CISO-as-a-Service
- Cybersecurity Strategies

Professional Services

- Security Services Implementation - WAF, PIM, DLP, EDR, DAM etc.
- Vulnerability Management
- Security Architecture Design
- Infrastructure Security Hardening
- Secure Cloud Migration

Our Flagship Products

FIRESEC

It is an automated solution for security device configuration analysis, optimization & compliance readiness. With Firesec you can determine compliance levels to PCI DSS, CI Security Benchmarks & other standards as well as determine insecure rules, redundant rules and unused rules that can help significantly optimise. We support most of the major firewall vendors, routers & switch vendors as well as the leading proxy products.

BlueScope
MANAGE . DETECT . RESPOND

It is an Elastic-powered big data platform for security analytics providing you the ability to mine massive amount of data, do pattern detection, threat hunting & advanced forensics. The use cases are mapped to the MITRE ATT&CK framework & enable detection of advanced attacks on your organization.

CONTACT US:

: US | India | Singapore | UAE

: info@niiconsulting.com

: www.niiconsulting.com