BANKING FRONTIERS

Vol. 19 No. 9 **January 2021** ₹75
Pages 52

www.bankingfrontiers.com
www.bankingfrontiers.live

TECHNOLOGY SUPPLEMENTS BOOST
CYBERSECURITY


SOURABH CHATTERJEE

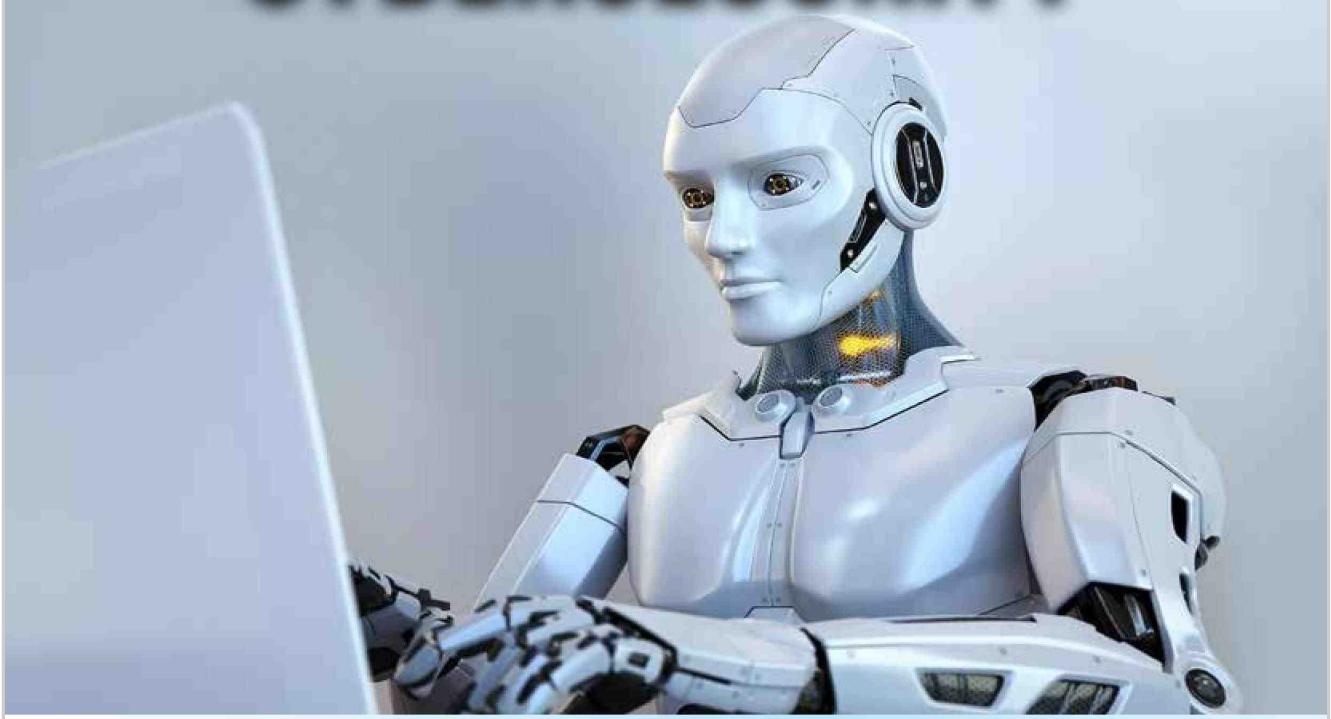

PAWAN CHAWLA


ANJANA RAO


KALPESH DOSHI


KIRAN BELSEKAR

TECHNOLOGY SUPPLEMENTS BOOST CYBERSECURITY



Banking Frontiers asked 5 BFSI technology experts about new approaches to improve information security in the light of growing attacks and frauds. We present their viewpoints in 4 parts spanning smarter approaches, emerging tools, updating process and people deployment.

Part 1

Intelligence as Force Multiplier

The risk and severity of cyberattacks have grown over the past few years. In fact, since 2018, organizations have witnessed the most horrific cases of cybercrimes related to massive data breaches, flaws in microchips, crypto jacking, and many more. The advancements of technology and the wide use of digital media are making attackers smarter by the day. Cybercriminals take advantage of individuals and firms targeting everything from a newly launched blog to an established website to gain access to sensitive information. A report by Threat Horizon, 2019 reveals that in the coming years, organizations will face cyberthreats under 3 key themes. The first is disruption as cybercriminals will use ransomware to

hijack technology devices and the IOT. The second is distortion, which is the spread of misinformation by bots and automated sources will cause a compromise of trust in the integrity of information. And the third is deterioration resulting from rapid advances in smart technologies and conflicting demands posed by evolving national security that will negatively impact an enterprise's ability to control information.

Says Pawan Chawla, CISO, Future Generali India Life Insurance: "We are seeing increased activity of cybercriminals and we are seeing sophisticated techniques used by them to circumvent traditional organizations' security tools. Organizations also face enormous challenges in the light of covid and the displaced workforces."

Sourabh Chatterjee, President & Head - IT, Web Sales & Travel, Bajaj Allianz General Insurance, maintains that it is a long-standing open secret that systems must be secure and most enterprises do not think of security as the first step. "Embedding security in the design of processes, architecture of solutions, and a part of daily operations is perhaps the most effective proactive measure for any enterprise. It is an active measure and the passive is protecting and detecting flaws, vulnerabilities in existing systems," says he.

TECHNOLOGY ENVIRONMENT

One of the essential things required to improve the information security team's efficiency is the skilling and reskilling of them. The other one is they need to have the right visibility to detect the anomalies in the technology environment that may trigger an incident and can be converted into a breach.

Kiran Belsekar, Chief Information Security Officer, Aegon Life Insurance, believes that if an organization uses DevOps or leverage cloud for innovation, then it can add security to the CI/CD pipeline and bring security to the left.

Sourabh says usage of artificial intelligence and machine learning increases the efficiency of information security teams. It also reduces manual tasks of detection and quarantine healing. Triaging

Sourabh Chatterjee advocates the usage of AI & ML for the infosec teams

critical incidents, hiring experts instead of generalists and correcting organization structure with proper developers instead of just auditors are all ways to boost the efficiency of information security teams, he avers.

ACTION NEEDED

Organizations need to understand manpower alone is not enough to cope with the ever-increasing number of cyberthreats. Security teams need to have a force multiplier to help maximize the use of their human intelligence and resources. Increasing efficiency requires 2 prospects: optimization of internal resources and an expert (internal/external) on hand to defend against the most advanced cyberthreats.

A force multiplier for operational security can be achieved through operational insight to obtain maximum resource value and gain a deep understanding of the current and desired level of security. Since one cannot be an expert to defend against the most advanced cyberattacks, there is need to involve a security expert.

Pawan recommends: "Identifying advance threats and automating intelligence responses and subscribing to various threat sources will help in detecting and protecting from the most advanced threats. One must automate correlation of data points using real-time threat intelligence for rapid identification and response. There is also need to empower the team through automation - automate actions that will help the security team to do more in less time."

Even today, if the organization follows basic security hygiene, they can prevent most attacks on their networks. The easy way to achieve this is by ensuring that one follows in spirit industry best practices, systems hardening and patching and a robust access control policy.

Kalpesh Doshi, CISO, FIS Global, believes that the principle of least privilege, multi-factor authentication for any remote access to organization networks or applications, regularly assessing your environment for known vulnerabilities and fixing them before the bad guy exploits the same cam help organizations to counter vicious attacks.

"The fundamentals of security will remain the same, hence you need a leader to steer your organization in these challenging times. I strongly believe that CISO is a leadership role, you can be a great manager or be strong technically but you can still fail. Also, the board and especially the CEO must LOVE (Listen, Oblige, Value, Empower) their CISO function to build robust organization security for their organization" says Kalpesh.

Part 2

Updating Internal Processes

There are multiple aspects of improvements, which can be brought to an internal process:

Organizations continue to experience cyberthreats that hold the potential to disrupt business operations and service to customers. A vast majority of those threats can go undetected, or they are detected too late for an organization to avoid exposure and the associated risk.

IMPORTANT MEASURES

In developing internal cybersecurity processes, it is not enough to prepare for the threats one believes one knows. One should also work to prepare for unknown threats. The hackers will continue to rise and one can find extreme sophistication in the tools and techniques they use to hack and achieve their goals. An organization needs to determine its crown jewels and the investment required to protect them. It is important not to prioritize the crown jewels based on a business continuity plan, but on considered risks.

Crown jewels can reside virtually anywhere - in the cloud, mobile or with business partners. An organization shall have a cyber threat intelligence (CTI) capability that will help in identifying, detecting and responding to threats. A proactive approach is required to seek new sources of information and new ways to interact with peers to identify trends and tactics. It is necessary to monitor and review logs and trails to gain insight and detect threats early. Also, it is imperative to make security awareness a priority - an awareness of threats, risks, challenges and solutions within every department inside your organization and within every partner organization. Besides, it is also necessary to explain the security challenges and rules in a language that employees understand. Awareness shall be more interactive, on-going and makes threats seem more concrete.

Anjana Rao recommends value stream maps to provide insights

Organizations know their critical assets that does not make them secure. Vulnerabilities are known to a hacker and known to the organization they target. Patch holes, focusing on critical holes as well as holes that might not seem critical but that are known.

Pawan advises that organizations need to be prepared for unavoidable: "Most organizations have a security incident management processes in place. But few have tested these processes. One must know how departments will work together during a cyberattack. It is important to know how you will engage regulators, partners and observers. Simulate incidents, bring in a

Says Sourabh: "I feel that ownership of improving internal processes should go beyond the CISO or the security team and its onus needs be taken by other stakeholders of the organization as well. Documentation needs to be detailed. Process documentation with detailing on security guidelines, procedures, etc. is a good beginning."

IMPROVEMENT PROCESS

There are multiple aspects of improvements, which can be brought to an internal process. When we look at a process to identify how we can improve upon the throughput, the journey starts with the following considerations:

- The objective of the process and its impact on business metrics and value chain.
- Ensuring what is the purpose of the process and identifying how critical it is in the value creation chain, who are the stakeholders which the process impacts, and which business metrics are impacted/controlled by the process performance.

This exercise itself at times leads to dropping a processor identifying the need to have a process to take care of the steps not being tracked.

Anjana Rao suggests some improvements in the process, checking the process performance, whether the process is delivering the desired outcome, and analyzing the variations in the outcome if any. The analysis of variation provides an insight into the opportunity for improvements and if the metrics need to be revisited, It will lead to identifying the avenues to optimize the process and reviewing the value stream maps. She says value stream maps always provide insight into eliminating wait time - owing to handshakes, reduction in TATs and capacity creation, automation of repetitive tasks, which means lower cost, more scalability, waste identification, meaning lowering the cost, optimal utilization of allocated resources, elimination of manual interventions, which will avoid repetitive tasks, risk mitigation and compliance to avoid operation losses and loss of repute,

ease of transaction, that is, simplifying processes, segregation of duties meaning workflow distribution, clear definition of process performance metrics, which is the unit of measure clearly defined with SLAs and reduce variations, which will drive consistency within and between processes.

Kiran points out that security is a moving target. He says it is important to impart principles of cyber hygiene to employees by imparting user training and measuring the efficacy of training and revisiting the internal policies like access management, vulnerability management, backup strategy, cyber crises response plan, security operations centre and having right KPIs. He also suggests getting covered under cyber insurance to safeguard against potential costly outcomes.

FOCUS ON SECURING CORE

Today there is this issue of information overload, which is creating blind spots that can prove fatal to an organization. There is, therefore, an urgent need to identify the organization's crown jewels and focus on securing the core the most.

Kalpesh feels that it is necessary to realize that we cannot and should not grant every organization asset the same level of importance. He cites the example of food, which is the most important and essential commodity and which still is not stored in safe vaults. "Similarly, CISOs will have to evolve and identify which of their assets needs the most security. These assets will be the ones which if compromised can have a catastrophic impact on the organization and challenge the very survival. There is a need for the risk-based approach to security decisions, not the other way. Risk treatment includes risk elimination, mitigation, transfer, and acceptance every risk cannot be eliminated or mitigated if you must even remain competitive in the marketplace," says he.

Part 3

Shifting Right People to the Right Job

Shifting of the ownership to empowered teams:

It is generally felt that cybersecurity is all about hacking into or breaking things, but cybersecurity in fact is all about learning how technology (and people) work. The key is not a technical background, but one's willingness and desire to learn how the technology works and to never stop playing.

PASSION TO LEARN

To ease the pressure on experienced people, one needs to bring in right people who have a passion to learn new technologies and understand how it works. It is also necessary to create automation in cybersecurity. The goal is to reduce the number of threats by eliminating vulnerabilities through the prevention of known threats and the identification of zero-day attacks.

According to Pawan, cybersecurity automation is also about making data collection faster and more efficient by bringing in artificial intelligence (AI) and machine learning (ML) technologies and processes into the fold to increase organizations' analytic capabilities, eliminating tedious, time-consuming non-cognitive tasks to free up IT security experts so they can focus on higher-priority RESPONSIBILITIES and tasks.

Kalpesh foresees great scope of RPA to shrink the demand and supply gap

Some examples of process automation solutions and platforms for cybersecurity include Robotic Process Automation (RPA), Security Orchestration Automation and Response (SOAR) and deep and dark web analysis.

Cybersecurity automation will ease the burden on senior resources and offer advantages in terms of being able to use security professionals most effectively. Using automation one can integrate security in the DevOps rituals and transform security to the Dev-First security approach. It is also necessary to shift the ownership to empowered teams.

Kiran says: "Survival of the fittest may work in the animal kingdom but grooming the less experienced resource requires a substantial investment of time, a sincere interest in employee development and a dash of humility."

HIERARCHY & AUTOMATION

Some of the things that can be shifted to people with less experience are day-to-day operations, repeat issues management and audit coordination. Sourabh says: "They can also take care of closure/documentation once critical incident and the overall approach are

defined and agreed upon and there is a clear implementation path. This will not only help them get their basics right but also free the more experienced people to tackle critical challenges."

With more automation, staff with lesser experience will be empowered to think outside the box. They will be enabled to manage processes and handle tasks like monitoring and managing process exceptions. Anjana Rao says: "Applying tools to perform root cause analysis and drive continuous process improvements will enable and provide access to standard operating procedures, which in turn will enable lesser tenured associates to take accurate decisions. In addition, there can be mentoring programs ('be my mentor programs') that can empower lesser tenure associates for taking up complex situations. This is like identifying high potential within the lesser tenure staff to fill in for the senior associates."

Currently, SOC is seeing an unprecedented increase in volumes of alerts that are generated by security tools. Kalpesh adds: "I believe there is a huge scope for RPA as the demand and supply gap for security resources is otherwise too wide. CISO teams must be battle-ready and hence, I believe every team member has an equally important role to play in securing organization assets."

IDENTIFYING CROWN JEWELS

In ideal situations, once an organization's crown jewels are identified, one needs to ensure that one has the best teams always monitoring them. Every organization asset is not critical hence new talent and upcoming leaders can be given those responsibilities to harness their skills and be battle-ready.

Part 4

Top Tools for Security

There is a growing variety of tools and methodologies for every problem:

Security tools are designed to perform various functions - from the endpoint and network protection to cloud security to identity and access control. The way threats are getting advanced, organization need to move from traditional security tools to highly advanced ones to protect the employees and the organizations.

IMPROVING PRODUCTIVITY

Cybersecurity is a team sport; it is the role of everyone. DevSecOps can play a crucial role in improving productivity by building automation and security gates, which will be a ShiftLeft approach. Kiran recommends closing the security loop faster and providing early feedback to the engineering team. "Do security as a code - writing code to automate the security," should be the mantra," says he.

According to Sourabh, productivity increases if the process is streamlined, standardized, automated and measured (to refine further). "I feel an end-to-end process coverage with tools for incident management, problem management, change management, etc, can bring about productivity improvement. Automation by the implementation of AI & ML can be leveraged to detect, quarantine, and heal," says he.

Pawan recommends EDR to enhance visibility into the endpoints

EFFICIENT TECHNOLOGY TOOLS

Security, Orchestration, Automation, and Response (SOAR) help an organization in streamlining security operations in 3 key areas: threat and vulnerability management, incident response and security operations automation. It helps in integrating and connecting various security tools and in automatic security operations.

The Dark Web is a home for hackers and terrorists and it could pose a threat to enterprises. If you find information about employees on the Dark Web, consider yourself lucky. It is better to know about this disclosure than to be unaware. There is nothing you can do to wipe out the information from other sites. However, this is a warning to tighten the network security and enforce a password change on all system users through the access rights management system.

Says Pawan: "Compared to traditional security solutions, EDR provides enhanced visibility into your endpoints and allows for faster response time. EDR tools detect and protect your organization

from advanced forms of malware (such as polymorphic malware), APTs, phishing, etc."

SIX SIGMA, OTHER METHODOLOGIES

IndiaFirst Life Insurance deployed a lean Six Sigma methodology to improve productivity and follows a DMAIC model (Define, Measure, Analyse, Improve, and Control). Anjana Rao, Chief Strategy Officer, at the company, says under each DMAIC phase, one can deploy an array of tools like define (KANO'S model, Project Charter, etc), measure (SIPOC, Gauge R & R, Sampling, etc), analyze (Ishikawa, FM, 5 Whys, array of statistical tools for hypothesis testing, Pareto's Principle), control (Impact Matrix, Box Plots, etc), improve (Poka-Yoke for warning, shutdown & control, learn tools, etc) and control (statistical process control, RASCI Matrix, cost-benefit analysis, etc.)"

Kiran promotes the training of the employees to maintain cyber hygiene

Kalpesh says organizations must remember that no single tool in the world can protect their organizations from all threats out there. The important thing is to build a security culture in the organization, which will form the basis for a strong foundation. Eventually, the tools and processes one implements in the organization will have to be one that aligns one's culture, priorities and skills availability. "A great security tool poorly configured is way worse than an average or even open-source tool configured optimally and where the teams have the skills to make use of every feature available in the tool. Productivity for security teams can be greatly enhanced by striking a balance between people, process, and technology," says he.

ravi@glocalinfomart.com