FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

INSIDER THREAT:

STAYING PROACTIVE AS COMPLEXITY GROWS

MARCH 2021
KLOGIXSECURITY.COM
617.860.6485

K logix

FEATS OF STRENGTH

INSIDER THREAT

MARCH 2021

FROM THE *Editor*

Dear Readers,

Protecting against insider threat has always been an integral part of any security program, yet with businesses rapidly transforming and environments increasing in complexity, the need for mitigation is increasingly important.

Many of the most damaging threats originate from trusted insiders who have access to critical and sensitive data within an organization, whether their intent is malicious, or they are acting negligently. While some organizations feel vulnerable to insider attacks, many of our customers and community of security leaders are aggressively taking action to address this concern.

We encourage customers to combat insider threat with a proactive mitigation program. They should identify and detect specific insider threats unique to their organization and environment, then assess and manage risk. It is important for leaders to understand how their businesses operate, identify core organizational goals, and recognize long and short term plans for growth to truly align their program with the business. An effective program protects the most critical assets and prevents impacts such as loss of revenue or intellectual property.

We recognize there is not a one size fits all approach to mitigating insider threats due to their complex nature. Transparency and flexibility are paramount as the threat landscape continues to evolve while businesses transform and technologies shift.

At K logix, we know insider threat programs span the entire organization, and all our offerings ensure alignment and consideration between business and information security. We meet customers where they are and have worked with organizations at all levels of maturity. We have helped organizations build a framework, set goals, roadmap initiatives and implement a strong insider threat program. We have also worked with organizations who experienced a recent insider threat incident or those who want to test the strength of their already robust program.

In this issue of the magazine, we hear from security leaders about their approach and experiences with insider threat. They share their thoughts on why the threat landscape continues to evolve and what may be done to stay proactive in a strategic manner.

I hope you find this issue of the magazine informative, and I look forward to hearing your feedback.

Kevin West

CEO, K logix

Magazine Contributors:

Katie Haug

Director of Marketing, K logix

Kevin West

CEO, K logix

Kevin Pouche

COO, K logix

Marcela Lima

Marketing Coordinator, K logix

About K logix: Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication *Feats of Strength*. Through hundreds of CISO interviews, we extract trends in order to provide services that align business to information security.

www.klogixsecurity.com/feats-of-strength

Marketing@klogixsecurity.com

ROSA FEYGIN

HEAD OF SECURITY
VISTAPRINT

HEADQUARTERS: Waltham, MA

EMPLOYEES: 6,000+

REVENUE: $1.4 Billion

Rosa Feygin began her career in the financial field, working in engineering, architecture, and developer roles, developing enterprise security solutions, which naturally compelled her to learn more about the information security side of business. Feygin says, "At certain points in my career, I decided that I wanted to go even broader into security to understand the policy, governance, risks, and risk management, and more from an organizational point of view to have that ability to grasp the bigger picture and understand how things work together between business and IT. That naturally made me think about moving into a CISO role."

Feygin held her first CISO role while at an independent bank corporation, which was both an educational and challenging opportunity, but one that enabled her to gain an immense amount of valuable experience. She learned how to develop secure applications, enable infrastructure, and proactively respond to audits and customers. Not only did she mature her business acumen, but she had the opportunity to report to the Board of Directors and communicate openly about risk.

At the beginning of 2020, Feygin took on her current role as Head of Security at Vistaprint, a Cimpress company providing marketing products and solutions. Feygin comments, "I decided that I wanted to move away from financial organizations and see how security is done in non-financial verticals. In my mind, security is not just a technical problem, it is a cultural problem. At Vistaprint, I work to make sure security is distributed across the organization and everybody has accountability for integrating security into their daily work and their business processes."

To date, Feygin has over twenty years of experience in information technology, information security, and risk management.

STRONG GOALS TO IMPROVE SECURITY

One of Feygin's top priorities is collaborating with their parent company Cimpress to strengthen the software development life cycle. She says to achieve this, they are focused on addressing any detected issues prior to production. Although many consider this basic security hygiene, it is vital for a functioning security program.

Feygin explains, "Right now we just introduced static code analysis to Vistaprint and it's going to be rolled out to all other businesses with the same purpose. But obviously there is much more than just a code analysis in a software development life cycle. We're also looking at the open source management, threat modeling and it's not that we don't have it, we have it, but we're trying to get it to a more mature state

where you can get to the level of consistency across all the tribes and all applications."

Another area of focus for Feygin and her team is incident response and making sure the company is resilient to cyber attacks and cyber threats. As threats become more sophisticated, they must detect as early as possible, then contain and respond in a productive manner. This may also include the help from various technologies relevant to their incident response approach and function.

To achieve their goals, Feygin fundamentally believes a strong security culture must be woven into each department and layer of the organization. She says, "A challenge which we've been addressing pretty successfully, and it's a never-ending process, is the security culture of the company. One of the most common attacks is credential stuffing that exploits and becomes easier to launch when passwords that are not complex enough or not stored securely. And this is what hackers exploit. As part of the overall security culture, to make sure that security is top of mind for every employee, if it's a technical employee or non-technical, they have to be informed. Security culture is definitely an ongoing challenge."

DESIGNING SECURITY BY DEFAULT AND BUILDING RELATIONSHIPS

As a business, Vistaprint is moving to the cloud and in order to ensure security is brought into strategic discussions around cloud adoption, Feygin works to establish strong interdepartmental relationships and meets at a regular cadence with all leaders.

She comments, "We are trying to move as fast as possible to be completely in the cloud. We must make sure that implementations are done by designing security by default. For automation, if there are any manual processes in place, there's always going to be an opportunity for inconsistency and it's difficult to manage and have visibility into how things are implemented. Security by default, where we can deploy through automation and we can detect any inefficiencies or insecure configurations through automation and then remediate, will get us to a much higher level of cyber resilience."

Feygin and her team strive to communicate regularly and proactively with other leaders to address business goals and understand the relationship between security and the business. She says, "Part of building strong relationships for me is to understand the highest business priorities each quarter. I must recognize what they need to develop or deliver to business partners and customers. And once they tell me a little bit more about what they are doing, then most of the questions are about how to make sure we meet all the security requirements and how my team can help enable them to deliver on time, but also with the appropriate security controls."

For Feygin, it is about finding a balance between the reputational risk, security risks, and making sure the business is not slowed down.

LEADERSHIP THROUGH COACHING

Feygin focuses on a coaching approach to leading and empowering her team. She tries to coach people and offer guidance while also affording them freedom to execute and explore. She tailors her leadership based on her team member's level of seniority and level of knowledge around security in order to enable strong and open lines of communication

She explains, "It's very difficult to get the skillset of people who have knowledge in technology and security right now in the market. So I try to balance this out and also organize the teams where the more senior people can partner with less senior people and they can provide the guidance for the less senior people and help them grow as well. So it's not just myself but the team as well."

INSIDER THREAT

Feygin says they address insider threats in many ways including through tabletop exercises and making sure Zero Trust is implemented. She comments, "Every year we have specific scenarios for red team exercises and this past year, it was an insider threat scenario. We dealt with an external consultant impersonating a newly hired internship student, who was trying to poke around, find weaknesses and exploit them in our environment. We also rely on Zero Trust, although that is not always enough. It's not just employees, it's also all our partners and vendors. And it's about not just the time they've worked for the company, but they might have left, and we need to make sure that all the access is gone."

A CISO'S PERSPECTIVE:
INSIDER THREAT - THE PROBLEM AND SECURITY MEASURES

BY ANDREW SMEATON, GLOBAL CISO, DATAROBOT

Cyber-defenders often focus on threats from outside an organization; however, the most damaging security threats originate from trusted insiders as they have legitimate access to computer systems, networks, and sensitive data. They often know precisely how the data is protected and can find ways to circumvent security controls, maintain persistence, and evade detection.

To add to the problem, remote work, during this pandemic, has opened up new insider threats. Many people have lost their jobs, and some are scared of losing. As a result, users might download their work files to an unsecured computer for future reference, which increases security risks.

Furthermore, remote employees might use their personal laptops and computers not protected by the organizations' security bubble, such as web gateways, intrusion detection systems, firewalls, endpoint protection systems, etc. This significantly increases the risk of data theft.

According to the insider threat report, 68% of organizations confirm insider attacks are becoming more frequent, and 53% of organizations believe detecting insider attacks has become significantly to somewhat harder since migrating to the cloud. In another report, the study showed that the average global cost of Insider Threats rose by 31% in two years to $11.45 million , and the frequency of incidents spiked by 47% in the same time period (from 3,200 in 2018 to 4,716 in 2020).

Insider threat is a multifaceted and multidisciplinary problem and is one of the most critical issues to combat where traditional security measures are ineffective. There are different types of insider threats:

- **Negligent insiders:** Negligence is considered the most expensive type of insider risk. Their intention is not to harm the organization but does so through inadvertent errors, carelessness, simply disregarding IT policies, or because of a lack of security awareness training. For example, they might open a phishing email or fall victim to a business email compromise scam.

- **Malicious insiders (disgruntled employees):** Insiders or third party with legitimate access who abuses their authority to harm the organization. Their goal may be to exfiltrate proprietary data or sabotage a company.

- **Collusive insiders:** In this case, malicious insiders are often found to work in collaboration to compromise the organization. It often involves fraud, intellectual property theft or a combination of the two. An example would be:

  Two employees of General Electric (GE) stole data on advanced computer models for calibrating turbines the company manufactured as well as marketing and pricing information. With the stolen intellectual property in hand, one of the employees started a new company and competed with GE in tenders for calibrating the turbines.

  What were the consequences?

  GE lost several tenders for turbine calibration to the new competitor. In 2020, after several years of investigation, the insiders were convicted and sentenced to prison time and $1.4 million in restitution to General Electric.

  GE employees downloaded thousands of files with trade secrets from company servers and sent them to private email addresses or uploaded them to the cloud. None of these malicious actions triggered a response from the

GE cybersecurity system. Deploying access management and user activity monitoring solutions could have helped GE detect intellectual property theft in time and speed up the investigation by gathering necessary evidence.

- **Imposters/Infiltrators:** Threat actors outside of the organization who steals the credentials of an authorized user and leverage that user's access to meet their objectives like exfiltration of critical/sensitive data.

Honestly, insider threats are harder to defend against than malicious outsiders. CISOs must prevent, protect, and prioritize the security threat from insiders as a part of a comprehensive security program. The program should be continuous and combine both technical and non-technical security controls. Cybersecurity best practices should be followed in general, such as candidate screening and hiring, onboarding and offboarding practices, security awareness training, and continuous assessment of security posture. In addition, a security policy for BYOD, remote work, IoT devices, social media, etc., should be established.

Another tip is establishing a very close relationship with your HR department. The HR department can often inform you of possible disgruntled employees.

Further, some of the key areas to focus on are as follows:

Identify and classify assets: The first step in asset security is to identify and classify information and assets as all the actions that follow depends on the classification. Determine the most valuable assets, their location, assess access criteria, and prioritize protection based on your organization's risk tolerance.

Implement separation of duties: the principle of least privilege, and job rotation: Separation of duties is ideal for protecting against collusion, which causes a deterrence effect. The principle of least privileges ensures that the insiders are granted only the privileges necessary to perform assigned work tasks and no more. It helps reduce the surface areas for malicious insiders. Job rotation serves two functions - First, it provides knowledge redundancy, and second, it reduces the risks of fraud, data modification, theft, sabotage, and misuse of information.

Use AI-powered solutions to monitor user behavior in real-time: An organization needs to invest in user behavior monitoring and analytics capabilities that provide visibility into people and assets and helps identify insiders who don't follow standard policy.

There are various tools available in the market that can be used in this context such as DLP, IAM controls, and SIEM with SOAR and UEBA (user and entity behavior analytics) integration.

Implement zero-trust architecture: "Never trust, always verify" is an ideal concept for more robust security. Zero trust eliminates the concept of trust as if the resources are being accessed by a stranger each time. With this implementation, we can prevent any unauthorized access to organization networks, resources, and data. It can also be used to granularly control what assets users can access.

Implement network segmentation: To combat insider threats, organization should implement intelligent network architecture using microsegmentation and Software Defined Network (SDN). SDN virtualizes network functionality and greatly simplified the management of an organization network. Microsegmentation creates secure zones in data centers and cloud infrastructure that allows the system administrator to isolate workload and limit network access based on a zero-trust approach.

Follow best security practices: Work with your HR department. HR-related controls can play a significant role, including vetting/background checks, execution of nondisclosure agreements, including during the hiring process, and active use of job descriptions in line with "need-to-know" requirements. Tip: make sure you compare the background check companies and have in-depth background checks on employees whom have key positions.

Follow global laws: Internal policies addressing requirements relative to the use of company equipment, devices and information assets must be in place. Organizations may significantly restrict the actual privacy expectations of employees by expressly excluding the private use of company assets. The GDPR requires companies to report a personal data breach to data protection authorities within 72 hours after becoming aware of it.

Insider threat monitoring software useability can only be used with strong business justification/ trade secret violation etc -- not as evidence of loafing.

Read the original version, published by Andrew Smeaton on LinkedIn

PATTY RYAN

CISO
ORTHO CLINICAL DIAGNOSTICS

HEADQUARTERS: Raritan, NJ

EMPLOYEES: 4,400

REVENUE: $1.8 Billion

Although Patty Ryan did not begin her career in security, in 2004 she was working at a financial services firm in the project management office and the CIO offered her the CISO role. With limited knowledge about security, she was required to leverage her problem-solving skills and strong business intelligence to lead a team of twenty security professionals. Since then, Ryan has held a number of different roles in security, working in finance, legal, and healthcare organizations.

Currently the CISO at Ortho Clinical Diagnostics (Ortho), an in vitro diagnostics organization serving more than 800,000 patients globally, Ryan oversees information and cyber security across the entire enterprise. She comments, "One of the things that hooked me in joining Ortho was the people. The process of talking to people through my initial job interview, I saw an amazing amount of transparency. I knew exactly what I was getting into, their personalities, the focus, the priorities, everything came out as part of that process, which allowed me to make a really informed decision in a very short period of time that doesn't normally happen as part of interviews. And they conveyed to me throughout this process a strong sense of partnership and a healthy appreciation for information security. So that sold me."

While interviewing for the role, Ryan was drawn to the opportunity to build and lead a security program as well as work in the unique field of medical devices. The challenge excited her, and she knew she would be able to not only mature the organization but grow her skillset while being supported by a strong company culture.

AN ORGANIZATION'S COMMITMENT TO SECURITY

The medical device industry poses unique challenges and Ryan works diligently to ensure her team continually enables the organization's commitment to delivering innovative, high quality diagnostics to healthcare entities around the world. Ortho's website highlights their commitment to cybersecurity by stating 'Ortho Clinical Diagnostics (Ortho) is committed to providing products designed with cybersecurity in mind and protecting all information that is entrusted to us by our customers.'

A key area of their commitment to cybersecurity is security by

> *"My job is to make sure that our products are secure while operationally simple so upkeep is not a burden to our customers. We don't contribute to their risk footprint."*

design. “My job is to make sure that our products are secure while operationally simple so upkeep is not a burden to our customers. We don’t contribute to their risk footprint,” says Ryan. By incorporating security into product design from the start, and throughout lifecycle management, threats are appropriately monitored and mitigated while meeting regulatory requirements.

TOP PRIORITIES

With an uptick in ransomware hitting healthcare organizations in 2020 and moving into 2021, Ryan says Ortho’s security team works hard to limit the risks presented by cyber criminals. She explains, “We make blood analyzers and clinical chemistry analyzers, and you think about the people who use our products. These are people who the toll of COVID has been amazingly high. Our products should not add to their stress level.”

Digital transformation is another area of focus for Ryan and her team as Ortho transforms its products and services. From a customer perspective, Ryan ensures the security needs are part of the conversation in every step of the way.

Ryan also considers looking back at core business functions to ensure security is fully functioning as an area to concentrate on this year. She comments, “You need to go back and look at your core business functions. You must a look at how to innovate and protect. For us, we continually review the level of risk present in different areas of our organization and make sure that level is acceptable. How do we mitigate, how do we understand what we know and what we don’t know in these environments? And how do we encourage transparency?”

CHALLENGES OF A COMPLEX INDUSTRY

Working in a complex industry such as medical devices poses significant challenges, and Ryan says focusing on security at a foundational level and not getting distracted by the latest trends helps her stay laser-focused on achieving her goals and protecting the organization.

Ryan explains, “From our product standpoint, lifecycle is a big challenge. From an idea to it being approved by a regulatory board such as the FDA, it could be three to five years. That is because of the amount of time it takes to build and completely test this complex infrastructure. Think about that from a security perspective, things move in days, weeks, and one design may be acceptable now, but is it going to be acceptable when we start verification and validation three or four years from now? So you must really look at security at a foundational level. Really stick with what you think are the tried-and-true best practices and means in which you can secure an infrastructure and really understand the evolution of the regulatory landscape and try to keep the bar at a consistent level.”

INSIDER THREAT RESILIENCY

Ryan says strong, resilient insider threat programs must be built on transparency with holistic visibility into behaviors and movement. While it is not the idea of ‘big brother’, it is vital to look across the environment whether it is Office 365, collaborating tools, or video conferencing and understand what employees are doing and where they have access.

Ryan explains, “I think the biggest issue with insider threat is the transparency or lack of transparency. Once you have the transparency, in my opinion, you can start building the rules and a logic that allows you to understand abnormal from normal. It is not easy and is a multi-layered approach.”

With increased numbers of remote workers, Ryan says insider threat has become an even larger security issue across the world. She encourages others to truly understand the flow, then compartmentalize how to handle the lockdown of each different area in an organization. She says, “The fundamentals have to be governed and when you start looking at locking down, it’s least privileged, need to know, and your businesses need to be part of the conversations.”

Insider threat as a service is a concept Ryan has heard about, where there may be an ability to buy an employee, so to speak. Bad actors could attempt to become trusted employees, especially with many recruitment interviews done over only a few video conferences.

From the strategic side, Ryan believes insider threat programs must continually align with business assumptions. She explains, “The business assumptions include who’s going to be using what data and how they want their data manipulated, how they want the data shown, where they want the data stored, where they need to have the data flow. How you then secure it, I consider far more of the people, process, technology, tactical side. Unless you have a really continued strong understanding of the business vision and tie an insider threat program to be able to reflect what the business needs, you’re going to have a problem of a lot of false positives or hiccups in the program.”

JOHN MANDRACCHIA

CISO
HEALTH PLANS, INC.

HEADQUARTERS: Westborough, MA

EMPLOYEES: 350+

REVENUE: $100.59 Million

John Mandracchia began his career working in IT as a second shift help desk employee at a local hospital in his early 20s. This early exposure to IT and the many components of working in that field, greatly interested Mandracchia and he continued to pursue IT as his career. Throughout his work in IT, he saw an emergence of work related to cybersecurity and eventually grew his career into that space. After working in various IT and security roles at hospitals, he then began working at Health Plans Inc (HPI), a third-party health plan administrator.

He explains, "I started at HPI in 2008. I had a career advancement opportunity that became available. I'd been at my previous company for 11 years. I loved it there as well, but with HPI, I fell in love with the organization because it was a smaller organization that allowed us to have exposure to a lot of different components that I hadn't had with larger organizations. The people that I work with are friendly, it's a diverse organization and everyone's so hard working, so it's kept me there for so long."

> *"...with HPI, I fell in love with the organization because it was a smaller organization that allowed us to have exposure to a lot of different components that I hadn't had with larger organizations."*

He began his work at HPI as a Systems Engineer and transitioned into a Team Leader for System and Infrastructure before taking on the CISO role in 2020. He says moving into a C-level role meant shifting away from being heavily focused on the technical day-to-day in order to address the managerial requirements as a business leader.

Mandracchia is responsible for protecting the confidentiality of PHI and PII while aligning security with the business. As with many smaller organizations, he wears many hats which include overseeing both the cybersecurity and infrastructure groups.

LEVERAGING THE CIA TRIAD

Mandracchia leverages the CIA triad of confidentiality, integrity, and availability of data to continue to strengthen his security program. By focusing on these key areas, Mandracchia implements high-level strategies that his team expands and executes on. He comments "A sub strategy of confidentiality could be to improve access control. A sub strategy of availability could be to mitigate something like a DoS vulnerability. Concentrating on these high-level methods have proven pretty well for me at HPI."

One of Mandracchia' s specific strategies for 2021 is to continue to strengthen their endpoints. He says because they are not working with just business computers or business networks anymore, their applications are becoming device agnostic and expanding across many networks. It is important for him to make sure the multitude of paths that lead to their data is manageable and secure.

In order to communicate the value of investing in endpoint protection, Mandracchia focuses on discussing risk with HPI's executives. He says, "It's a lot of risk evaluation and weighting risk. If there's multiple components to our network, we go through them and pinpoint the ones we feel are becoming higher risk. We communicate that process by going back into our risk assessment process and showing why we think something has changed. We're expanding desktops, we're making applications device agnostic, we need to make sure that we can portray that on paper, the increase in risk."

Like many other security programs, Mandracchia says resources are often a key challenge. He explains, "Similar to how real estate is location, location, location, for us it's resources, resources, resources. I define resources as employees, equipment, skills, experience, utilization of products, services, and so on. Where I work at HPI, the organization has had continuous growth year after year, and with that growth, you have a demand for increase with those resources. But the challenge with growing efficiently is to address those growth demands while keeping costs manageable so you can keep being competitive in a competitive market."

SHIFTING PRIORITIES

Mandracchia says their disaster recovery plan helped them through the many changes brought about by 2020. The strong plan in place with their disaster recovery program provided a framework to easily adapt to dramatic changes, such as those that sprang up with a newly remote workforce. He remarks, "I'm fortunate to report to our CIO, who I've been working with for 13 years, and we've always gone through every connection possible from switches onsite, routers onsite, network connections, everything is pretty much redundant. We always try to have a fail over plan. All of our employees from day one of the pandemic were working remotely and of course we had some issues with connectivity, stuff like that, but really the biggest change that we noticed was the communication demand."

This communication change required their organization to identify how they can continue to stay in touch in a productive and efficient manner. Mandracchia states, "We realized Microsoft Teams is pretty much a front facing application for all of the Microsoft products and since we're heavily a Microsoft shop we saw it as a win-win and we could eliminate our costs for Zoom and GoToMeeting. Now it is how do we implement it? How do we utilize it? How do we make sure people aren't going to over-utilize it and put PHI on there? It took us a little while to get the Teams platform implemented but as I said, we immediately recognized there was value for it, but getting it in place was the priority."

"Similar to how real estate is location, location, location, for us it's resources, resources, resources. I define resources as employees, equipment, skills, experience, utilization of products, services, and so on..."

PHI AND THE CONSIDERATION FOR DATA

In the PHI protection industry, including healthcare, health insurance, and other related entities, Mandracchia says becoming more granular with data identification will only become more important and prevalent. He comments, "We're seeing such a rise in regulations and regulating bodies such as GDPR and CCPA. Health Plans is a company that started in New England and is looking to expand nationally. And as we expand nationally these regulations are going to be prevalent. And the regulations are very aggressive when it comes to being very specific with items like data mapping. It's not only being able to map data and map the flow of your data, but the ability to carve out any single person, certain attributes of a person, pretty much at the request of the customer."

They must ensure their data is mapped well with an ability to focus on cherry picking exactly what they want to remove from data, wherever it resides. Mandracchia says the challenge is there may be legacy systems or smaller level SaaS providers that cannot autonomously sift through legacy data with a command or script to remove the individual or attribute.

INSIDER THREAT

Mandracchia says it does not take a technically minded individual to penetrate an organization and become an internal threat in today's world. Employers must extend a level of trust to their employees and also place the right controls in place, such as strong access controls, damage may be minimized, according to Mandracchia. He continues, "The simple fact remains that if anybody who has a camera, which is widely accessible, can capture data and extract that data, it's not that difficult to achieve. I can't speak as to why there would be a rise in insider threats themselves, that would be pure speculation, but I can say that it's a concern and it should be a concern for most organizations."

INSIDER THREAT:
THE VALUE OF A PROGRAM-FIRST APPROACH

By Katie Haug, K logix

IN 2021, ANALYSTS PREDICT:
33% OF ALL INCIDENTS WILL BE DUE TO INSIDER THREATS*

PROGRAM FIRST, TECHNOLOGY SECOND

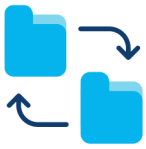
Having a solid approach and defense against insider threat starts with implementing a strong, strategic program. Many times, security leaders jump to investing in a new technology to address insider threat, without an adequate program in place. This may result in insufficient protection and an ad hoc approach without considerations for business requirements.

On page 8, Patty Ryan (CISO, Ortho Clinical Diagnostics) explains, "I think the biggest issue with insider threat is the transparency or lack of transparency. Once you have the transparency, in my opinion, you can start building the rules and a logic that allows you to understand abnormal from normal. It is not easy and is a multi-layered approach."

The risk around insider threat is rising as corporate environments increase in complexity. On page 10, John Mandracchia, CISO at Health Plans, Inc. says it does not take a technically minded individual to penetrate an organization and become an internal threat in today's world.

IN 2021 AND BEYOND, INSIDER THREATS ARE A FOCUS ARE DUE TO:

Rapid shift to remote work – harder to detect insider threats in the cloud



Increased ease of moving stolen company data via cloud, e-mail, network attached storage, USB, etc.

Employee job insecurity due to financially impacted organizations

Considerations for employees' privacy & state-driven policies around privacy – keeping humanity of employees top of mind

THE PANDEMIC'S IMPACT ON INSIDER THREAT

An increasing number of remote workforces, accelerated cloud migrations and even recent breaches such as SolarWinds have added layers of complexity to insider threat as many organizations are losing varying levels of visibility and control.

On page 6, Andrew Smeaton (Global CISO, DataRobot) says – "Remote work, during this pandemic, has opened up new insider threats. Many people have lost their jobs, and some are scared of losing. As a result, users might download their work files to an unsecured computer for future reference, which increases security risks. Furthermore, remote employees might use their personal laptops and computers not protected by the organizations' security bubble, such as web gateways, intrusion detection systems, firewalls, endpoint protection systems, etc. This significantly increases the risk of data theft."

INSIDER THREAT IMPACT

The top three impacts of an insider threat incident are:

Operational disruption or outage

Organizations are deeply affected when outages or operational disruptions occur, including brand, financial and resource-related effects.

Loss of critical data

Sensitive and critical data is the lifeblood of many organizations and must be protected across the entire organization.

Brand damage

Reputation and customer trust weigh heaviest when brands are damaged through an insider threat.

Other impacts may include legal liabilities, loss in competitive edge, or loss in revenue.

EFFECTIVE INSIDER THREAT PROGRAMS

According to CISA**, successful insider threat mitigation programs employ practices and systems that limit or monitor access across organizational functions. Those practices and systems, in turn, limit the amount of damage an insider can do, whether the act is intentional or unintentional.

In every case, effective insider threat mitigation programs need to be able to detect and identify improper or illegal actions, assess threats to determine levels of risk, and implement solutions to manage and mitigate the potential consequences of an insider incident (CISA).

Many organizations may view insider threat programs as costly and resource-exhaustive, due to considerations such as legal and privacy concerns. However, security leaders must ensure they leverage existing skillsets within their teams and evaluate or operationalize any technology that may add insider threat coverage. They must also clearly articulate to business leaders the impact of an insider threat and justify the resources required to build and maintain a robust program.

According to CISA, effective insider threat programs:

- ☑ **Identifies and focuses** on those critical assets, data, and services that the organization defines as valuable
- ☑ **Monitors behavior** to detect & identify trusted users who breach the organization's trust
- ☑ **Assesses threats** to determine the individual level of risk of identified persons of concern
- ☑ **Manages the entire range of insider threats,** including implementing strategies focused on the person of concern, potential victims, and/or parts of the organization vulnerable to or targeted by an insider threat
- ☑ **Engages individual insiders** who are potentially on the path to a hostile, negligent, or damaging act to deter, detect, and mitigate

Sources:

*Cybersecurity Insiders. "2020 Insider Threat Report." https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf

**Cybersecurity and Infrastructure Security Agency. "Insider Threat Mitigation Guide." November 2020. https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485