Cargill® Helping the world *thrive*

Annual Cybersecurity Report

An insider's look at protecting Cargill

2022

A message from Chief Information Security Officer, Jim O'Conner

It's been a year of non-stop action in cybersecurity.

In FY22, we saw our competitors' names in the news for cyberattacks, shutting down their supply chains and prompting our businesses to ask, "Could that be us?" We saw Cargill services impacted by successful attacks against our third-party vendors, hindering our ability to conduct basic business processes, such as time tracking. Throw in the worst vulnerabilities we have ever seen and add in a war. This is our threat reality.

This year we focused on the most effective steps Cargill can take to protect and recover our assets in the event of a successful cyberattack. Accelerating this work across the breadth of Cargill is strengthening our technology and operational resilience, driving assurance that together we are taking the right steps to address our threat reality.

Along the way, strategic investments in governance, asset management and manufacturing are paying off. These investments are helping us accomplish more despite the increased cyber activity. We have matured our approach to setting clear expectations for managing risk, and our path to remediating vulnerabilities is clearer and quicker.

While I'm eager to share our successes, thank our businesses for their partnership and share our stories of innovation, what I also hope shines through in this report is the talent, resilience and commitment of the people of Technology Governance, Risk & Control. Through a challenging year, we remain guardians of our mental health and rally to support one another, regardless of the challenge.

Jim

Advancing our Cyber Foundation

Enabling faster and safer growth through governance

Knowing if we're doing the right things to protect Cargill from cyberattacks starts with governance. The more organized and disciplined we are in our approach to governing cybersecurity, the more confident we can be that we are acting in the best interest of the business.

Continued maturity for governance programs and assessments

TGRC's governance programs matured their foundation in FY22 by continuing to refine framework and control expectations, how we measure progress, provide assurance and even how we onboard governance programs. Two new governance programs were introduced in FY22: malware security and identity and authorization. Control self-assessments for applications, which were started in FY21, are giving us a better view of risk. We can holistically analyze gaps for all applications by feeding the results from the first assessments back into our governance programs and shining a light on needed adjustments.

Getting an outside opinion

Program assessments by independent external parties are a hallmark of good cybersecurity oversight. TGRC doesn't rely solely on internal expertise but works closely with external partners to measure program progress, benchmark with similar industries and bring strategic insights to our program roadmaps. Bringing the outside in helps us adapt more quickly to risks from new technologies and our ever-evolving threat reality.

64,650 employees and contractors who were assigned *Data Privacy and Cybersecurity annual refresher* training

85 requests for information about our cyber program from regulatory, government and customer questionnaires, audits and assessments

1,235 library of responses for information requests, reduced by 40% this year, helping us consolidate and sharpen responses

Preparing for cyber attacks

Cargill continues to be at risk for cyberattacks. Protecting our data and systems and assuring our ability to recover from a successful attack was a priority focus in FY22. Across the company we accelerated work to strengthen our resiliency, prioritizing the most effective actions. Here's where we focused for the greatest impact:

Preparing our businesses

[redacted]ness to adapt quickly to disruptions and maintain operations, they must [redacted]d the possible impacts of a cyberattack by working through a Business [redacted]alysis (BIA) and testing their Business Continuity Plan (BCP) to keep the business up and running.

[redacted]% of Cargill's businesses and functions have a BIA to identify their critical [redacted]ss capabilities, a 61 percent increase from last year.

[redacted]our backups

[redacted]st crippling aspects of certain types of cyberattacks, like [redacted] the ability to get your data back. Backups are a key foundation of resiliency. TGRC is helping define the ideal state for our backups so we can get our data back if attacked.

[redacted] Managed Global IT windows production servers set up for [redacted]ups.

Reducing our attack surface

Our attack surface is where we are vulnerable, and simply by doing everyday business, Cargill provides criminals plenty of ways to attack. It's our connections to third parties, computer devices, software and services that provide attackers a way in if they are left vulnerable. The goal here is to fully understand these areas and apply consistent configurations to reduce risk.

[redacted] Operating System vulnerabilities remediated – a 75% reduction

Managing MADJVs

As Cargill enters merger, acquisition, divestiture and joint venture (MADJV) activity, a significant amount of technology change is introduced to our environment. Criminals often target companies during times of transition. Managing MADJV activities in a more structured approach helps us protect our investments and operational capabilities.

[redacted] MADJV engagements with heavy involvement from TGRC teams, including Information Security and Enterprise Risk Management.

Access to Cargill assets

Who and what can access our network, connect to our systems and login to our sites and services takes careful consideration. Prioritizing critical areas and ensuring modern protections are in place makes the difference between a criminal gaining unauthorized access or being stopped at the door.

[redacted] Unique (MAC) addresses checked as they try and connect to Cargill.

Effective and deployed controls

[redacted]s aren't just a good idea, they are the backbone of good IT. Once in place, [redacted]ed to work as expected. If a control deviates from its intent, we need to know and automatically get it back on track. Missing or broken controls that present immediate risk must be identified for triage and remediation.

[redacted] Various devices, applications and servers continuously monitored controls.

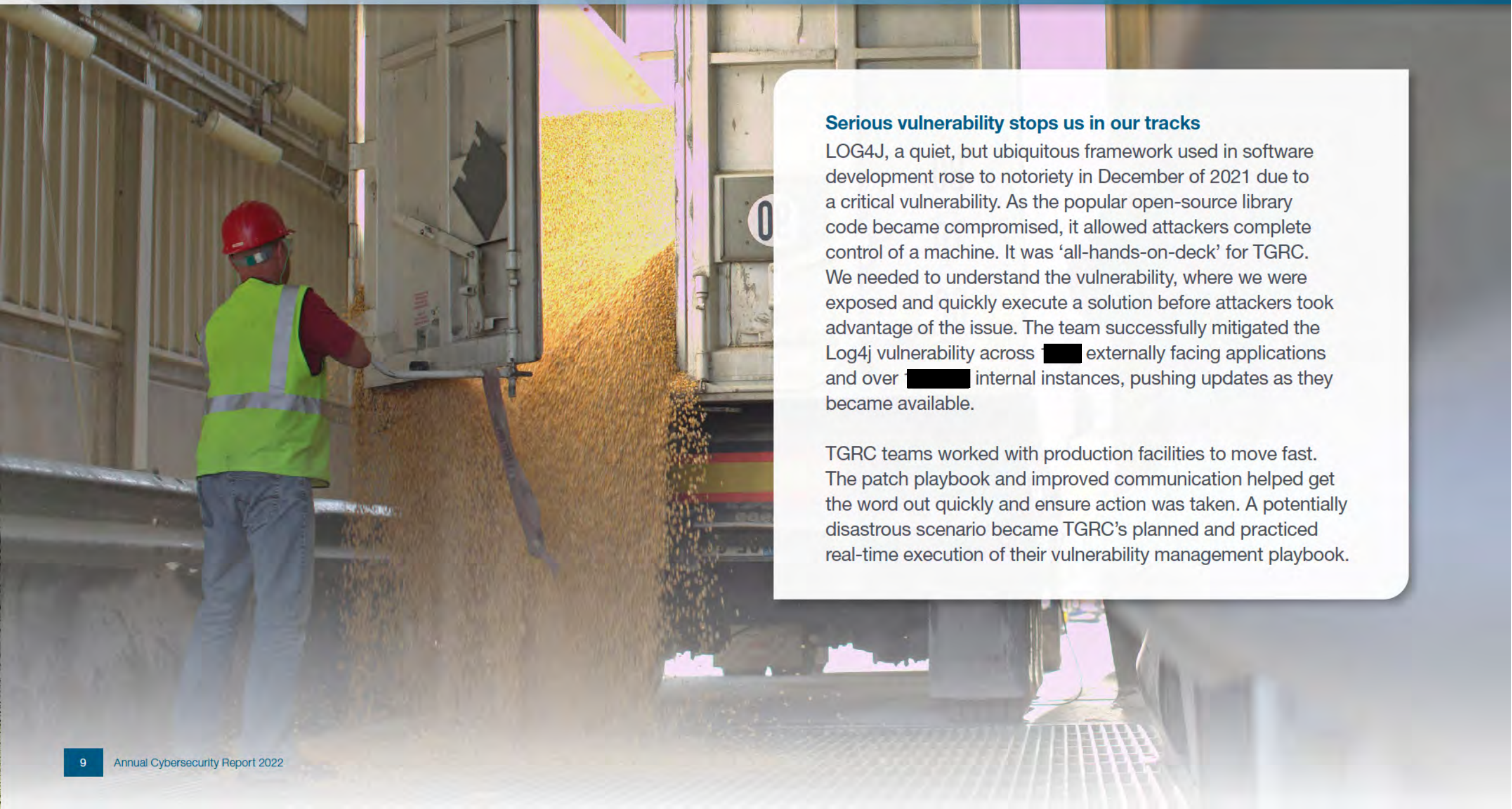
[redacted]

When attacks happen – the reality of cyberattacks

Beef industry takes notice of cyberattacks

When a competitor's beef plants shut down due to a cyberattack, the world's food companies took notice. The attack exposed supply chain vulnerabilities and reinforced the reality of ransomware attacks. Cargill's protein businesses took quick action for each of their sixty plants. In came an integrated solutions team (IST) who did individual plant assessments and plans. The team created a protein playbook with an interactive online site for crisis management response and support. The playbook helped identify unique location information along with critical requirements, giving Protein a path for swift and decisive action in the event of an attack. Now, if the facility or systems go down, the business' investments in redundancy and high availability technology provide greater assurance of recovery.

Protein's partnership with TGRC provides the preparedness needed to be in the driver's seat, ready when needed.



Serious vulnerability stops us in our tracks

LOG4J, a quiet, but ubiquitous framework used in software development rose to notoriety in December of 2021 due to a critical vulnerability. As the popular open-source library code became compromised, it allowed attackers complete control of a machine. It was 'all-hands-on-deck' for TGRC. We needed to understand the vulnerability, where we were exposed and quickly execute a solution before attackers took advantage of the issue. The team successfully mitigated the Log4j vulnerability across [redacted] externally facing applications and over [redacted] internal instances, pushing updates as they became available.

TGRC teams worked with production facilities to move fast. The patch playbook and improved communication helped get the word out quickly and ensure action was taken. A potentially disastrous scenario became TGRC's planned and practiced real-time execution of their vulnerability management playbook.

Crisis plans in action

Seeing the likelihood of war in Ukraine, TGRC put its own resiliency planning into action to understand the risks and prepare for impacts.

With businesses and customers already on alert from recent cyber events, their quick understanding of the crisis response needs led to a combined team preparedness and proactive efforts. From understanding impacts to creating and testing continuity plans for possible scenarios to rehearsal and collaboration with regional crisis management teams across the globe - Cargill was ready to take action.

Teams dug in to understand assets per location in Ukraine and Russia, learning about operating systems, business purpose, type of equipment and criticality. They worked with Ukraine employees, as they attempted to escape the country with their laptops, to have them disabled until they reached safety and verified their identity.

TGRC's partnership with the business, combined with a sustainable process, allows us to analyze and prioritize risk to meet our business resiliency needs and ensure an appropriate approach to maintain business operations during a crisis, and most important – protect our people.

Protections for now and the future

Using intel to predict threats

Our Cyber Command Center teams are working together to add intelligence-driven analysis to threats against Cargill. Combining contextual information about our adversaries to indicators of compromise, gives us a holistic approach to cyber risk detection and moves us from reactionary to predictive approaches.

An intelligence-driven workflow allows insights to become immediately actionable, providing transparency, agility and flexibility. As the team acquires information or a cyber event requires a direct action, they gather the details, including indicators of compromise, malware repositories, how criminals are taking advantage of a vulnerability, etc. This information is put into the system so all involved can see the details and actions taken to provide instant collaboration and communication.

Knowing if our third parties take cybersecurity as seriously as we do

Our third parties are helping fuel Cargill's business growth, providing great value. TGRC works with our businesses to know our vendor's and strategic partner's cybersecurity posture and practices, so we have a level of assurance they take cybersecurity as seriously as we do. But attacks happen, and we must take steps to protect our environment from becoming a casualty of a third-parties' cyberattack. Reducing the attack surface from vendor connections is one way we mitigate the risk. This approach was taken to better protect personal information within SAP, which communicates with many non-SAP systems. The team deployed remote function calls (RFC) to thwart an attacker from being able to remotely execute malicious code, which could allow full control of an SAP instance.

Remediating vulnerabilities 24/7

When a security researcher accidentally leaked details of an unpatched Microsoft vulnerability dubbed PrintNightmare, Microsoft was quick to push out a patch, but it only fixed part of the vulnerability. Attackers could still gain broad system privileges. The TGRC Cyber Threat Detection and Response team dug in over a holiday weekend to develop, build, test and validate a custom solution to solve this high-risk vulnerability and shut the door to attackers.

TGRC adopts an agile methodology

Moving to an agile methodology has benefited teams across TGRC, especially in how we prioritize our work. Teams are taking a structured approach to get work done, whether it is a new security solution or a continuous improvement. An agile approach gives us more control of our focus and productivity.

[redacted]
application scans for vulnerabilities

[redacted]
attributes used to enhance threat detection

[redacted]
security alerts handled – everything from malware to hacking

[redacted]
Drop in Java vulnerabilities globally

Collaboration, innovation and automation

Helping our Joint Ventures mature their cyber posture

Cargill invested in an agriculture technology company, Bushel, to provide software technology solutions for growers, grain buyers, protein producers and food companies. Bushel's interactive portal receives transactional data from Cargill, so farmers stay informed with prices, contracts, transactions and more. As a young company just getting started, Bushel needed help ensuring secure data and getting up and running safely.

Partnering with CASC, TGRC embedded a dedicated resource into Bushel's data security team to help prepare the organization with the fundamental security controls before launching their product. This security expertise gave us confidence that they have the processes, systems and controls that keep our data secure.

Throughout the engagement and ongoing, TGRC shares best practices, helps reduce risk and increases speed to delivery, providing value to all involved.

"TGRC's personnel investment helped close technology gaps for privacy and security, reducing risk, accelerating business case achievement, and helping our customers be successful."

– [redacted]

Learn more about Bushel on **Cargill Connects**.

Access control automation for our banks in hours, not months

Thousands of applications throughout Cargill require regular cleanup to ensure access is removed as people leave, change roles or no longer require access. Manually reviewing these accounts one by one would be an ongoing and time-consuming task for businesses. Intelligent Robotic Process Automation (RPA) can automate this task and remove countless people-hours.

Cargill-managed banks, with about four thousand users, had never been reviewed for appropriate access, putting Cargill at risk for data privacy compliance, regulatory, and financial and reputational implications. To rectify this, the TGRC team developed two RPA bots to reduce the gap: the first captures each bank profile created, and the second reviews accounts to confirm it is an active user. Now, when someone leaves who has access to an account for one of Cargill's banks, it takes less than 24 hours to remove their access when it previously took months.

Automation saves time and money while boosting morale

The Development Operations (Dev-Ops) team within Identity and Access embarked on a systematic approach to build products that simplified self-service for Cargill IT teams and end users. A typical Single Sign-On request averaged three months to complete, and with over a hundred requests per month, the process was inefficient and often a frustrating experience for all. Soliciting feedback from the business with monthly demos and honest conversations, the team worked to transform their offering from a disparate set of tools to a self-service, automated product with simplified instructions. The new SSO automation shrinks requests to completion to minutes, allowing the business to realize connections faster and giving TGRC's team more time to build and innovate, providing value-add products that boost morale and their skillset.

[redacted]

of data hosted on our internal document review platform

[redacted]

third-party engagements managed

[redacted]

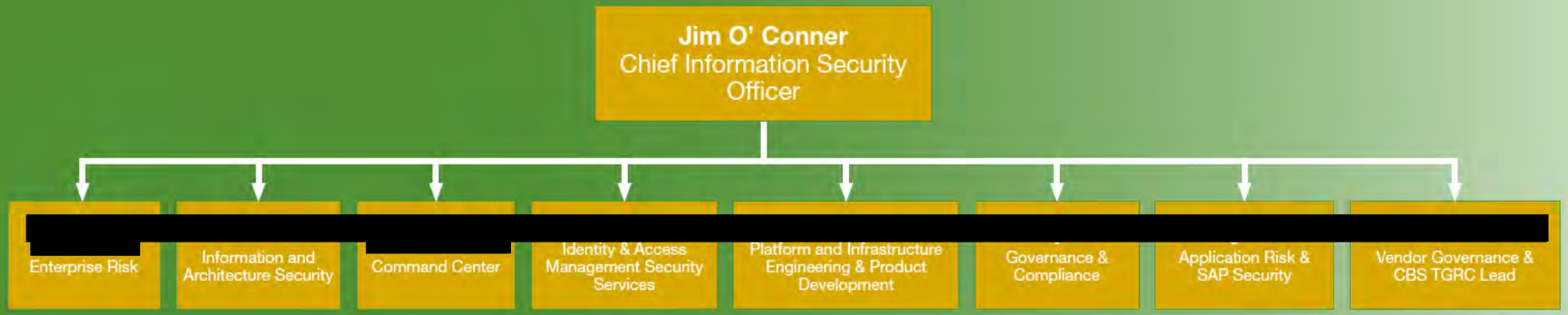
projects completed by the Enterprise Risk Management team

[redacted]

Reduction in technology debt and unnecessary services

Our People

Meet the team who leads Technology Governance, Risk & Control



TGRC Partners Closely With:

- All Cargill Enterprises and Functions
- Global IT
- Global Ethics and Compliance
- Global Privacy Office
- Financial Controllers Organization
- Internal Audit
- Plant Operations
- External regulatory groups
- External information sharing forums

TGRC Role Spotlight: Enterprise Risk Management

The Enterprise Risk Management (ERM) team serves as the primary connection point into our businesses and functions globally. They help identify and analyze cybersecurity risks that come from doing business. They look at the risk of third-party connections or a new software-as-a-service application or the need to collect personal information from our customers – these risks are managed through early involvement in projects and initiatives. The team partners to protect what is most important to the business, keeps them informed of threats and drives a security-positive culture that ensures appropriate controls are implemented and maintained.

Business Information Security Officers or BISOs, a key role within Enterprise Risk Management, are focused on building a stronger connection to the business and achieving deeper conversations around cybersecurity risk. As a result, it's easier for businesses and functions to see a clear path to managing cyber risk.

"The team is talented, passionate and driven. Every day they are helping our businesses achieve their growth goals and be customer driven, but in a way that considers our collective cyber-risk, so we can adapt fast and grow."

– [redacted]

Allies for mental health

When you are a team responding to crisis, you often live in a heightened state of tension for long periods of time, and it can take a toll on your mental health. TGRC takes the health of its people seriously and puts our people first, knowing burnout is a very real factor of living in prolonged states of crisis and threat. We lead with kindness and support each other by listening and sharing resources to help find balance.

Bringing the outside in and giving back to the community

The secret to a strong cybersecurity culture is leveraging knowledge across industries and throughout the cyber ecosystem. Our TGRC team takes learnings from the outside to better Cargill and continues to share their knowledge and expertise with the outside to help create a safer cyber world. Here are a few examples.

[redacted] vendor governance and CBS TGRC lead, is a member and past Executive Council participant of the Information Systems Audit and Control Association (ISACA) Bangalore, India chapter. She has also driven initiatives to promote the importance of women in cybersecurity, including the Women in Tech program and university outreach. She co-leads the Cargill Women Network in India, mentors as part of Cargill's cohort scholarship program and supports returning mothers through the Diversity, Equity and Inclusion (DEI) council.

[redacted], policy consulting and management advisor, is a chairperson for WG05 of the ISA99 cybersecurity committee for plant systems. [redacted] subject matter expertise helps ISA99 address industry-wide industrial automation and control system cybersecurity concerns, whose compromise could result in impacts such as endangerment of public or employee safety, loss of confidential information, economic loss and more.

[redacted], business information security officer for Cargill Protein & Salt, is a committee member of the North American Meat Institute's (NAMI) cybersecurity committee. Started in September of 2021, the committee discusses cyber topics impacting the industry and advises on cyber standards. Participation allows Cargill to collaborate and learn in a non-competitive way with protein businesses, large and small.

[redacted], identity and access operations manager is a Certified Information Systems Security Professional (CISSP). Certified by the International Information System Security Certification Consortium, or (ISC2), which is a non-profit organization that specializes in training and certifications for cybersecurity professionals. A challenging certification demonstrates high-level cybersecurity expertise and requires continuing professional education credits (CPEs). [redacted] is one of a handful of TGRC employees who holds and maintains this certification.

[redacted], risk and security manager for EMEA, is a board member of the overseas security advisory council (OSAC). This board organizes seminars on cybersecurity, presented by national and international speakers of industry, government and military. [redacted] is also a member of the ISAC of the Port of Amsterdam and working to expand and include Rotterdam to his memberships.