CHRISTOPHER HUDEL

christopher@hudel.com
linkedin.com/in/chudel

PROFESSIONAL EXPERIENCE

SPREEDLY

Chief Technology Officer (CTO) *2021 – 2024*

Wholly and holistically lead the engineering department (application engineering, infrastructure, architecture, information security, IT) through significant 50% y/o/y growth. Accomplishing "all the really fun things" a Chief Technology Officer would expect to do at a late-stage startup: doubling an engineering team, driving resiliency and scalability forward within the environment, partnering with "at scale" customers, working together with partners on big-wins, leading forward with DEI through example, and sponsoring awesome and fun hackathons.

- **Operations Excellence**
  Drove improvements in process and technology that resulted in 9 months (2022) at-or-better SLA vs. previous year (2021), trailing twelve months at 100%. High-scoring DORA metrics in deployment frequency, lead time for changes, mean time to recovery, and overall change failure rate, while consistently hitting "high water marks" in managing requests/per/second throughput and overall API transaction growth.

- **Major Tech Initiatives**
  Architected and oversaw implementation of a new cloud-native data pipeline between the core transaction database and downstream (reporting, warehousing, billing) systems, replacing a bespoke multi-hop process with a single direct-to-Kafka connection in the process. Lead the team in migrating from a legacy unsupported DB technology to a newer highly available (CockroachDB) database without requiring planned downtime or maintenance. Stewarded implementation of a DR capability in secondary Amazon region.

- **People Leadership and Team Growth**
  Doubled the engineering team size within the first twelve months while simultaneously increasing employee engagement scores by 7%. Crafted and communicated individual contributor and engineering manager career pathing (honoring both technical and managerial ladders), demonstrated high cohesion with corporate DEI initiatives through hiring, brought forward successful first-ever nearshoring relationships, and lead with seasonal hackathons that accelerated both innovation and bug-fix initiatives.

Chief Information Security Officer (CISO) *2020 – 2021*

As the inaugural CISO, establish an information security practice that seeks to defend and protect a robust global payments orchestration platform responsible for vaulting over 1 billion payment card details and through which flows over 50 billion (USD, 2024) in gross merchandise value annually. Inclusive of annual successful PCI and SOC-2/Type-2 certifications.

FIRST CITIZENS BANK *2017 – 2020*

VP, Principal Information Security Architect

Design solutions that protect, detect, and respond to cyber and criminal threats that would otherwise impair a ~$35B regional bank operating in over a dozen states with a sizeable digital footprint. Reporting to the Information Security Officer.

- **Architecture**
  Discover opportunities and design / implement solutions that make for better banking customer (both commercial and retail) experiences in a secure manner. Solution development includes the following: deployment of a new online banking multi-factor authentication solution (and roll-out in 6 weeks to all commercial banking customers), and customer Single Sign On (CIAM) among all lines of business.

- **Vision & Thought Leadership**
  Facilitate creation of annual Board of Directors Information Security update and strategy design sessions, leading to a 24-month information security strategy, embracing emerging technologies (SD-WAN, Mobility, Big Data, Cloud) within IT and the business.

- **Cyber Fraud Response**
  As part of a "SWAT" team, develop and rapidly deploy custom anti-fraud detection and response capabilities for loss prevention in the areas of wire transfer, account takeover, and ATM transaction fraud.

XPO LOGISTICS *2015 – 2016*

Chief Information Security Officer (CISO)

Develop and lead a globally accountable team of 20+ information security professionals, protecting $15B in revenue across multiple countries and all lines of business. Reporting to the CIO.

- **Information Security Program Creation**
  As the inaugural CISO, develop a global information security program, multi-year strategy road-map and execute tactical necessities while developing a global team. "Quick-win" deployments included the implementation of: multi-factor authentication, reduced attack vector for lateral movement, security information and event management (SIEM) platform, multilingual education & awareness materials, and cloud-based secure web gateway and firewall infrastructure.

SPX CORPORATION *2011 – 2015*

Chief Information Security Officer (CISO)

Reporting to the CIO, accountable for enterprise information security across multiple business segments spanning 30+ countries, 350+ locations, and 14,000+ employees. Executive leadership actions include the domains:

- **Strategy & Vision**
  Developed an 18-month strategy whose execution was subsequently accelerated in a 12 week timeframe to significantly augment the corporate capabilities to prevent, detect, and respond to advanced, persistent, cyber threats. New and augmented security uplift included: multi-factor authentication, consolidation of prolific Active Directory environments, consistent and rigorous system/application patching, perimeter-based web/email malware detection and prevention, risk-based password policy management, privileged-access management, endpoint device control, and vulnerability management.

- **Advanced Persistent Threat (APT) Forensic Analysis, Incident Response & Remediation**
  Lead the investigative and incident response/remediation efforts addressing an emergent nation-state-sponsored cyber threat. Efforts involved cooperation and collaboration with US Federal law enforcement and external counsel.

- **Service Design, Execution, and Support**
  Implemented two separate projects to a) provide new service capability (multi factor authentication) and b) improve existing service capability (replace internet proxy technology). Delivered projects on-time, within budget, and complete with a transition-to-sustain model for level-1 and level-2 support on the go-live date. Services consumed by 7,000 and 10,000 customers respectively.

- **Vendor Management**
  Created and oversaw multiple Requests for Proposal (RFP) processes across over a dozen vendors for multi-year, multi-million dollar service contracts providing managed Security Information & Event Management (SIEM) and 24x7x365 security operations center (SOC) services. Negotiated annual attack and penetration test vendor selection and contracts. Performed critical 3rd party information security risk assessments.

- **Executive Relationships**
  Presented regularly in quarterly briefings and ad-hoc meetings with business presidents. Responsible for providing updates to members of the corporation's Board of Directors, consistent with National Association of Corporate Directors (NACD) published guidelines. Responsible for reporting to executive management the status of a new multi-year strategy to adopt the NIST cyber controls framework (based on the critical security controls).

- **International Relations**
  Working with colleagues and partners from across the globe, provided biannual updates at "IT All Hands" meetings with information specific to each geography. Met regularly with colleagues from USA, Germany, UK, France, and China, working together to deliver solutions to meet both corporate and regulatory (i.e.: Works Councils) requirements.

- **Education & Awareness**
  Managed and provided scheduled and on-demand Information Security education and awareness training to both general and targeted audiences. Mediums for delivered content included in-person, webinar, video, blog posts, "break room" posters, and internal newsletters.

- **Risk Assessment and Design Review**
  Performed risk assessment for new Software as a Service (SaaS) offering under development within an SPX business unit. Assessment was inclusive of operational, cyber, and business risks inherent in the new offering, addressing operational readiness and maturity alongside PCI, cloud computing, and 3rd party supplier risk

EDUCATION & CERTIFICATIONS

UNIVERSITY OF WATERLOO
Bachelor of Arts (BA)

GLOBAL INFORMATION ASSURANCE CERTIFICATION (through 2028)
GIAC Security Expert (GSE)
GIAC Experienced CyberSecurity Specialist (GX-CS)
GIAC Experienced Incident Handler (GX-IH)
GIAC Experienced Intrusion Analyst (GX-IA)
GIAC Security Essentials (GSEC)
GIAC Certified Intrusion Analyst (GCIA)
GIAC Certified Intrusion Handler (GCIH)
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
GIAC Mobile Device Security Analyst (GMOB)

OFFENSIVE SECURITY
Offensive Security Certified Expert (OSCE)
Offensive Security Certified Professional (OSCP)

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP®)
ISC2 · Certificate # 21575 (2001-2023)

PRESENTATIONS & SPEAKING EVENTS

SELLING YOUR IDEAS UP AND WITHIN YOUR ORGANIZATION
Private Hosted Engineering Event

RANSOMWARE: WHAT EVERY GROWTH COMPANY NEEDS TO KNOW
Spectrum Equity Hosted Event

VALUE OF CROWDSOURCED SECURITY TESTING
FS-ISAC Expert Webinar Series, Internet

SECURITY ISSUES IN SOFTWARE DEVELOPMENT SUPPLY CHAIN
Hacker Horizons Webinar w/Synack, Internet

POOR USABILITY: THE MOTHER OF INVENTION
BSides Charleston, Charleston, SC

CYBER SECURITY AND WAYS TO PROTECT YOUR BUSINESS
Chamber of Commerce, Charlotte

ANATANOMY OF AN APT ATTACK
NC Infragard, Raleigh

NATION-STATE ATTACKS
Defense Industry Cyber Threat Working Group (DI-CTWG), Atlanta

COMMUNICATING EXTERNAL THREAT & RESPONSE
NC Infragard, Charlotte