Managing Cyber Risk

Eliminating the Blind Spot

Our Security Mission Statement

We help organizations align security with strategic business objectives, creating an information security program that is integrated into your business. With today's threat actors continuing to evolve their tradecraft by employing more advanced and evasive techniques, **it's all about mitigating risk.**

Security & Risk Consulting:

Assess, enhance, and design security programs that strengthen your security posture

Our Security & Risk Consulting practice provides a broad portfolio of services to address the information security, risk and compliance needs of our clients. Our IT security consultants help clients:

1. Identify vulnerabilities and assess real business risk.
2. Meet PCI, NIST, GDPR, HIPAA, GLBA, FISMA, ISO 27002 and other security compliance frameworks / mandates more efficiently and effectively.
3. Devise security and governance programs that fit a client's environment.
4. Help them recover from, and prepare for a cybersecurity breach.

Cyber Security Myths:

Organizations commonly mistake the following as evidence of adequate security

- **We have never been attacked, so our security is good enough:**
  Security threats are constantly growing in complexity and sophistication and perpetuators can be dormant for considerable periods.

- **Security is well-managed by the IT department:**
  IT should not be solely responsible for managing cyber security. A security incident can have significant and long-lasting effects for the entire business. Therefore, it's important for business leaders and the IT department to manage cyber security together.

- **We have invested in a high-end security tool:**
  Security tools are only fully effective if they are correctly configured and appropriately monitored, maintained and integrated with overall security operations; and one tool cannot prevent all security threats.

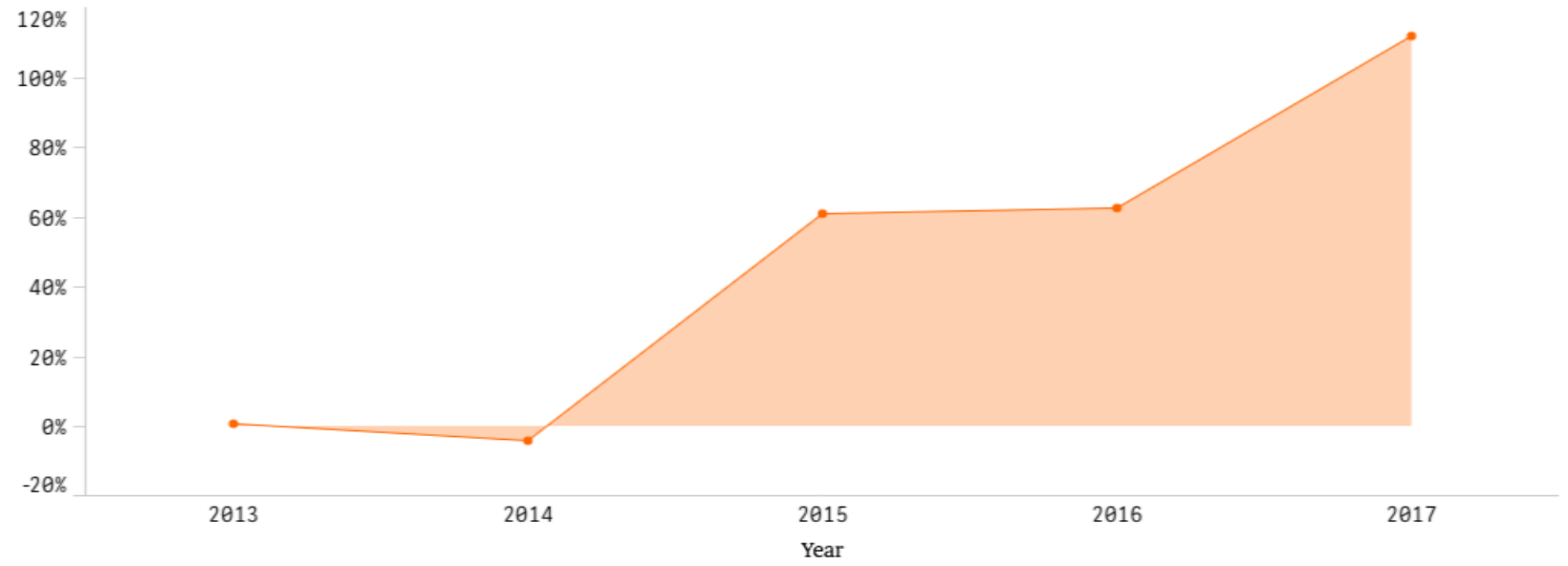
Cyber Security Facts & Figures:

Cyber Loss is on the rise in professional services organizations…

Chubb Percentage Claims Growth - Last Five Complete Years

All Industries and All Revenues

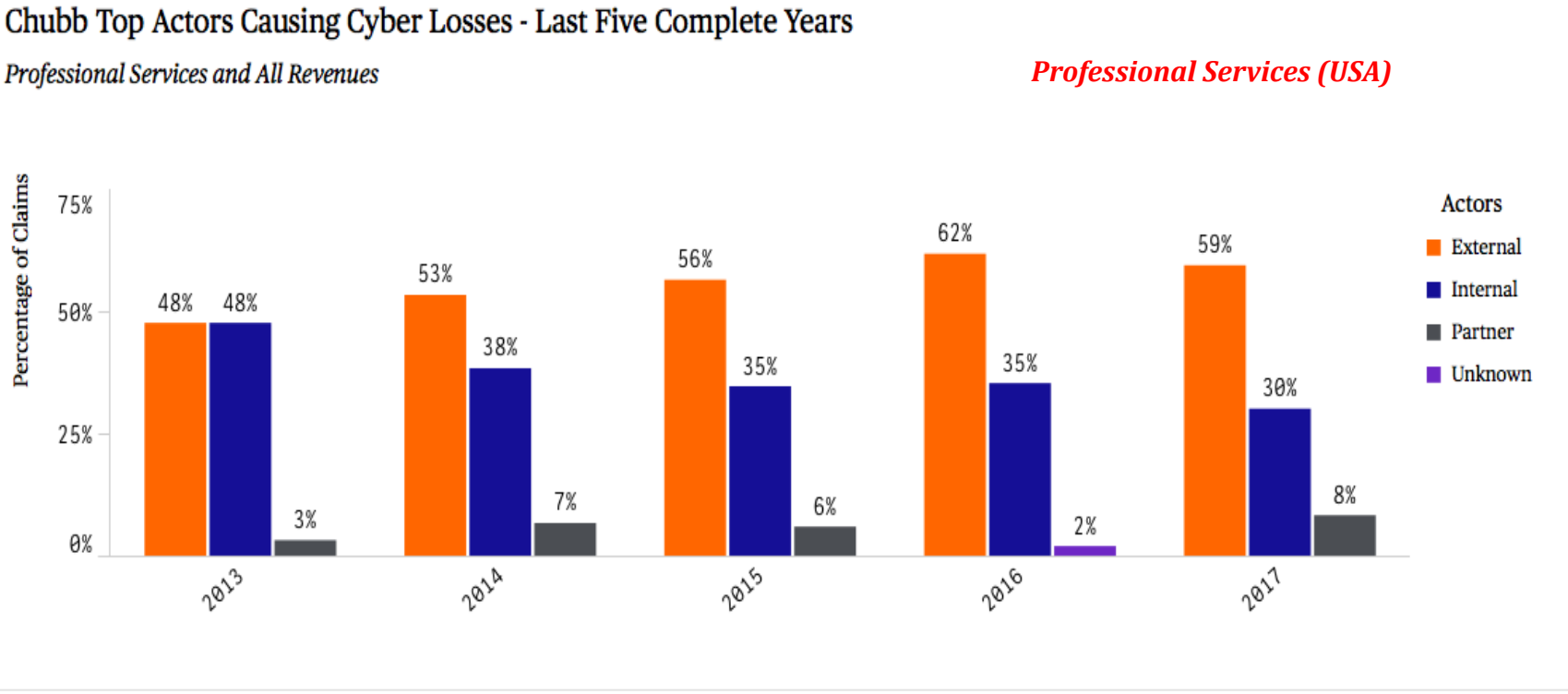
Professional Services (USA)



CHUBB

Cyber Security Facts & Figures:

External Actors Continue to be the Largest Threat…



Cyber Security Checklist:

Can you answer these questions about your organization?

MANUFACTURING CASE STUDY- Part I:

We have the correct insurance coverage - or do we?

Spoofing and phishing are part of what is known as social engineering fraud. Social engineering fraud is typically a type of computer fraud where an employee is misled into believing he or she is communicating with a vendor and is tricked into sending money due that vendor to the fraudster. Many organizations take proactive measures to protect themselves through enhanced IT measures, employee training and the purchase of computer fraud and other types of cyber insurance.

BUSINESS DILEMMA: A recent district court action in Washington illustrates how social engineering works and highlights the importance of understanding the limitations of the types of insurance coverages companies may have:

- A hacker began to intercept the email exchanges and sent fraudulent emails using “spoofed” email domains that appeared to a seafood importer to be “actual” emails.
- The hacker substituted the “1” for a lower case “l” so it looked legitimate. In one of the emails, the hacker directed the seafood importer employee to change the bank account information for a vendor for future wire transfers.
- The seafood importer's employees made the changes as directed and transferred **$700,000** in payments to the new account.

MANUFACTURING CASE STUDY-Part II:

We have the correct insurance coverage - or do we?

NEGATIVE BUSINESS OUTCOME:

- The seafood importer submitted a claim for the misdirected wires under its Wrap and Crime Policy, which specifically covers computer fraud. **Its claim was denied on the basis of an exclusion to the policy, which precluded coverage for loss resulting directly or indirectly from the input of electronic data by a natural person having the authority to enter the insured's computer system.**

- **Because there was no unauthorized use of the seafood importer's computer system, coverage was deemed not to apply. The district court's ruling is consistent with similar precedents.**

- The case is currently on appeal before the 9th U.S. Circuit Court of Appeals**.**

BUSINESS SOLUTION: (2 prong approach)

- **Risk Management -** As social engineering fraud becomes more prevalent, human vulnerabilities are a high cyber security risk. Creating a data governance policy, implementing security best practices and conducting an annual penetration test will limit exposure.

- **Risk Transfer** - The seafood importer did not have correctly structured cyber insurance (narrow coverage language). A annual & comprehensive review of insuring agreements, i.e., Broad Liability Coverages (Media/Network Security/Privacy Regulation, etc.), Reimbursement Coverages (Extortion, Social Engineering, Privacy Event) will eliminate risk.

LAW FIRM CASE STUDY:

Legal Jurisprudence demands that lawyers protect the confidentiality of their client discussions & information

BUSINESS DILEMMA:

A mid-sized law firm had a data-privacy breach caused by the relentless hammering from outside threat actors - human hackers or automated bots. The incident involved illegal access to information stored on the law firm's servers, which may have included information relating to sensitive personal information, trial transcripts, and financial records.

BUSINESS SOLUTION:

CyberSearch, Ltd. implemented a layered security defense to further strengthen the law firm's existing safeguards, starting with vulnerability testing services comprised of wireless & network penetration testing, social engineering testing. This was followed by end user education & awareness training — improving its threat intelligence and defensive posture.

BENEFITS:

- Gained extra protection against threat actors
- Validated client confidentiality assurances
- Improved visibility to overall security effectiveness & reduced threat response times
- Raised threat awareness among management and staff

Portfolio of Services:

We offer a complete portfolio of cyber security services to help you define your strategy, identify threats and risks, deploy the right technologies and ensure…

As your security partner, we'll assess your existing information security programs and develop, implement and manage customized information security protocols through the following services:

1. **Security Program Strategy:**
   - Address gaps, manage risk and develop a roadmap to mature your security initiatives
2. **Threat and Vulnerability Management:**
   - Uncover weaknesses & remediate threats and vulnerabilities
3. **Governance, Risk and Compliance:**
   - Collection of services designed to create, adapt and operationalize a security strategy that addresses your organization's most likely threats and top risks while remaining accountable to business objectives
4. **Security Education & Awareness Training:**
   - Educate & train employees about how to safeguard data and protect company resources

CONTACT

With our quality credentials and experienced team, and our proven methodology, we are confident that ITConundrums, Inc. is the right choice to partner with you.

ITConundrums, Inc. Contact:	David Siegler CEO
Telephone:	224.433.7970
E-mail address:	dsiegler@itconundrums.com