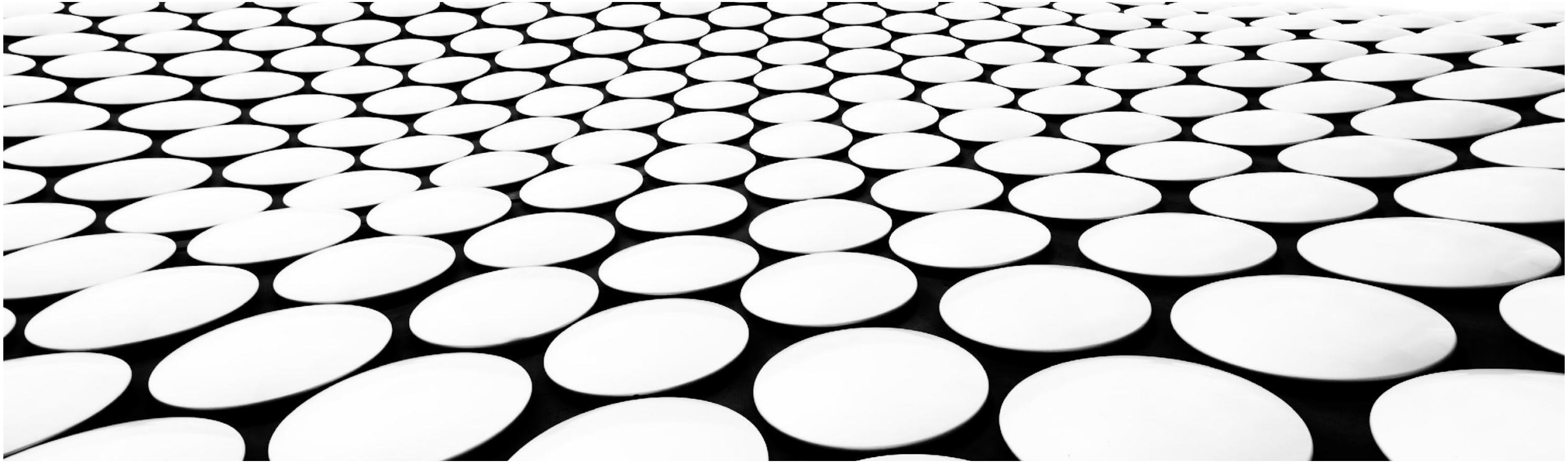
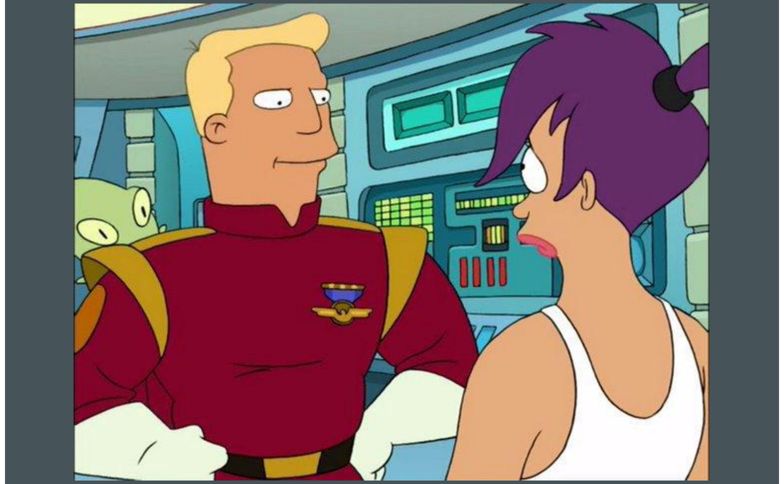
CYBER LIABILITY INSURANCE

A CUSTOMER’S PERSPECTIVE BY KEELAN STEWART



KEELAN STEWART



Has my fame preceded me or was I too quick for it?

CISSP® GLEG GICSP

HCISPP® GSTRT CIPP US SANS Security Awareness Professional

About the Speaker

- Bachelor and Master degrees in Information Assurance from University of Nebraska Omaha
- Myriad of certifications
- Head of GRC program for Boys Town

Disclaimer: I am not an attorney and do not represent any insurance company. This presentation is strictly my personal experience and views on cyber liability insurance as a customer on behalf of an organization.

ENSURE ≠ ASSURE ≠ INSURE

Ensure

Ensure: to make certain that something shall occur

- Involves taking an action, i.e., implementing security controls
- HIPAA 45 C.F.R. Part 164 § 164.306: “Ensure confidentiality, integrity, and availability for ePHI…”

Assure

Assure: to declare earnestly; to guarantee

- Involves trust and a basis for believing the assurance, i.e., documentation, certification, audits
- CJIS 28 C.F.R. Part 20 § 20.1: “It is the purpose of these regulations to assure that criminal history record information…”

Insure

Insure: to arrange for compensation in the event of damage to or loss of property, etc.

- Involves transferring risk to another party for a fair market value
- Mass. Gen. Laws § 93H-2: “Insure the security and confidentiality of customer information…”

CORPORATE INSURANCE

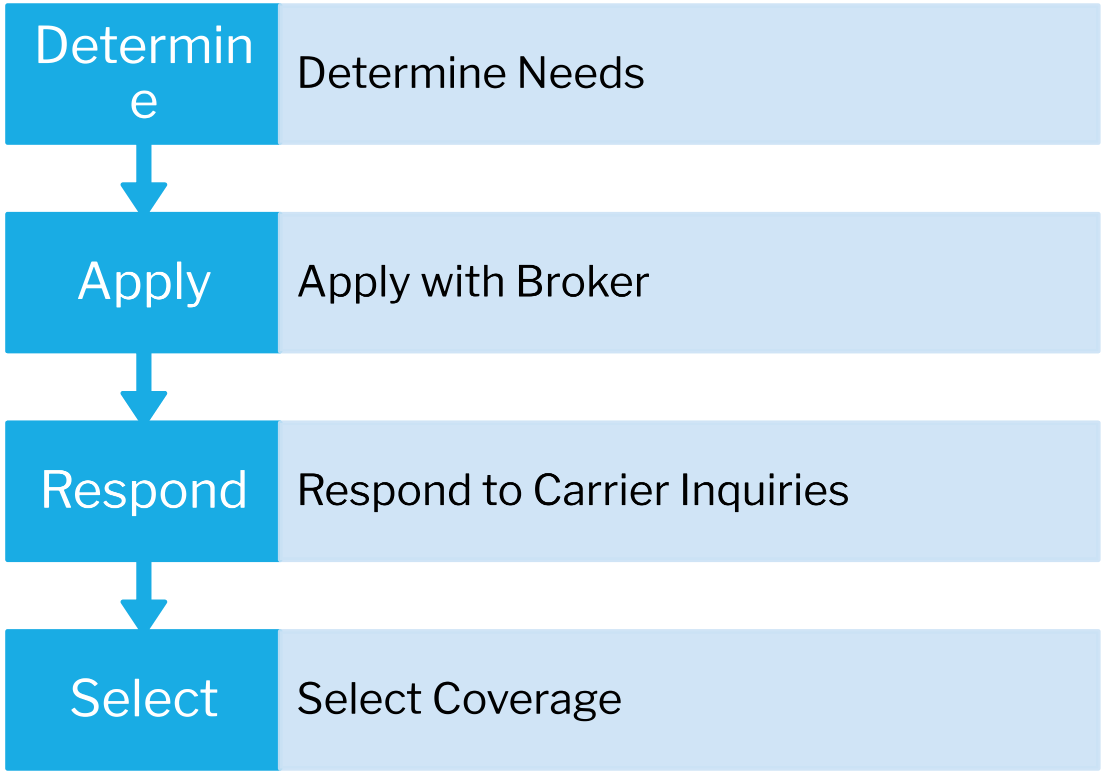
Some General Types of Insurance

- General Liability
- Contractual Liability
- Automotive Liability
- Statutory Workers' Compensation
- Umbrella or Excess Liability
- Commercial Crime
- Professional Errors and Omissions (E&O)

Some Types of Cyber Liability Insurance

- Cyber Liability (all encompassing or with carve-outs)
- First-Party (expenses and losses)
- Third-Party Liability
- Ransomware

OVERVIEW OF PROCESS



Determin
e

Determine Needs

Apply

Apply with Broker

Respond

Respond to Carrier Inquiries

Select

Select Coverage

- A broker works to understand your organization and needs, then works with carriers to get you the desired coverage
- Carriers sell specific insurance coverages based on actuarial evaluations of perceived risk, which vary based on the carrier, their specializations, your organization's posture, and the threat landscape
- Any residual, uninsured risk remains the burden of the organization and is effectively self-insured

DETERMINE NEEDS

- Contractual Requirements
- Board Expectations
- Security Posture
- Self Insurance

APPLY WITH BROKER

Do not lie

Any misrepresentations will not be covered, so it doesn't help you any

Plus, it's just a bad look

Gather accurate data

This will be difficult, time-consuming, and cross-departmental

Start early

Ask questions

Your broker is your representation to the carriers and will assist with technical jargon, scope, etc.

RESPOND TO CARRIER INQUIRIES

- Time
  - It will take time for your broker to solicit bids from a variety of carriers. Try to give them as much time as possible before your renewal window so you can get as many bids as possible.
- Vetting
  - Carriers will vet you using the broker survey, third-party monitoring services, and external scanning tools to identify as much exposure as possible.
- Inquiries
  - Many carriers will ask specific follow-up questions, either regarding something on your survey or something they discovered during their due diligence. Again, be as honest and transparent as possible to ensure you do not misrepresent your security posture.
- Remediation
  - Some carriers will discover specific, technical issues, such as an external vulnerability, and allow you to remediate them before they bid on your coverage. Take advantage of the free external scans and utilize any third-party monitoring services against your own domains.

SELECT COVERAGE

Your broker will present you with all bids received on your requested coverage.

- You may need to select coverage options from multiple carriers
- You may also need to establish more realistic expectations with leadership

Once you select your carrier(s) and coverage, familiarize yourself with the benefits of your plan

- Digital forensics
- Penetration testing
- Information sharing

PROGRAMMATIC READINESS

GAP ASSESSMENTS

Use your insurance renewal as a gap assessment. Plan to have bandwidth to remediate simple findings and document projects that require resources.

Turn your own third-party due diligence tools and processes on yourself. Try to keep all externally-facing scorecards with passing grades. If you are a vendor to large organizations, ask if they can send you their reports on you.

Make sure your leadership understands that cybersecurity is the cost of doing modern business. You can either pay that cost up-front to put in security controls or on the backend in fines and increased premiums.

RISK MANAGEMENT

Systems of Record

Know how many unique records of each protected data type you have

PII, PHI, PCI, Financial, FERPA, HR, Privileged, IP, etc.

All Systems

Know architecture, authentication, encryption, etc.

Enterprise Security Controls

Know configuration

NARRATIVES

- Breaches & Incidents
  - Maintain detailed documentation
  - Seek counsel before releasing details
- Maturity
  - Keep a list you update quarterly of new technology, staff, programs, etc.
- Events
  - Write a brief account of how you respond to any newsworthy events
  - Anything event your board would ask about, have a canned narrative for your broker

CONCLUSION

- Cyber insurance has become a form of accreditation
- Insurance supplements, not replaces, a strong security program
- Use your insurance renewal process to mature your organization
- Perfect is the enemy of good