Information Privacy & Industry Impacts

cieca

Collision Industry Electronic Commerce Association

CCi Global Technologies

Brandon Laur

Vice President, Client Experience

- 12 Years at CCi, started straight out of school.
- BA in Marketing & Organizational Behavior.
- Various positions from Support to Development.
- Facilitating industry groups for 10+ years.
- Passion for the ACE and the people within it.

CCi Global Technologies

Steve Driz

Chief Information Security Officer (CISO)

- Over 25 years of hands-on experience bridging business and technology
- Bachelor in Computer Science, and Executive MBA from the UofT
- Prestigious professional designations - I.S.P and ITCP by the Canadian Information Processing Society
- Exposure to information and cybersecurity from the early 90s
- Help variety of key executive positions in various industries
- Contributed to the success of several start-ups in the Fintech industry

CCi Global Technologies

Formerly know as ClaimsCorp

Vision:

respect - collaboration - trust

To be the most trusted source for data aggregation, analytics, and performance improvement for the valued stakeholders in the auto claims economy.

Locations:

Head Office:	Hamilton, ON
Regional Offices:	Stoney Creek, ON Vancouver, BC Milton Keynes, UK

Digital Product Suite:

- Secure Data Interfacing
- Solution Integration
- Business Intelligence
- Tailored Software Services

Information Privacy & Industry Impact

1. Cybersecurity
2. Automotive Value Chain Impact

First, what is Cybersecurity?

Cybersecurity is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber attacks.

It aims to reduce the risk of cyber attacks and protect against the unauthorized exploitation of systems, networks, and technologies.

Important Components

Data

Information translated into a form that is efficient for movement or processing.

Policies

How you collect data and what you can do with it.

Cyber Security

What you do to protect unauthorized access/use of the data.

Data Privacy and Security Trends - 2021

- Working remotely has increased exposure
- Authentication Abuse
- Insider Threats
- Ransomware Attacks
- Supply Chain Attacks
- Zero Trust
- The need for Extended Detection and Response (XDR)
- Cyber Insurance

Data security is more important now than ever before as we face a number of challenges.

- Data is the world's most valuable resource and is at the core of business operations.
- Data volumes in need of protection are growing at explosive rates.
- Data creation, processing, and storage are increasingly done at growing complexity and making data flows harder to track.
- Ever-greater computing power and artificial intelligence are widely accessible, allowing cyber criminals to target businesses more effectively than ever before.
- Any organization that uses modern day technology must acknowledge the risk of cyber threats, which is why addressing this risk is more crucial than ever before for the health and operation of businesses.

Breaking down "The Data"

Two types of data:

1. **Personal Identifiable Information**

   Any data that can be used to identify a specific individual. Technology has expanded the scope of PII considerably. It can include an IP address, login IDs, social media posts, or digital images. Geolocation, biometric, and behavioral data can also be classified as PII.

2. **Machine-to-Machine**

   Any data that is produced from the direct communication between multiple devises using any communication channel.

…each have their own set of standards and best practises.

But what about our industry… how does this affect us?

Collision Industry Data Usage:

- Both PII and Machine-to-Machine data are at risk.
- Various producers and consumers of data.
- We have an evolving ecosystem of data movement.
- No clear ownership of data.
- More and more connected devices.

What about the buzz around GDPR and Data Privacy?

GDRP = General Data Protection Regulation

Protection Principles:

1. **Lawfulness, fairness, and transparency:** Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation**: You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. **Data minimization**: You should collect and process only as much data for the purposes specified.
4. **Accuracy:** You must keep personal data accurate and up to date.
5. **Storage limitation**: You may only store personally identifying data for as long as necessary for the specified purpose.
6. **Integrity and confidentiality**: Processing must be done in such a way as to ensure appropriate security
7. **Accountability**: The data controller is responsible for being able to demonstrate GDPR compliance.

Data

Information translated into a form that is efficient for movement or processing.

Policies

How you collect and what you can do with the data.

Cyber Security

What you do to protect unauthorized access/use of the data.

Hacking used to be for fun, now it is for profit.

How do we protect ourselves?

Recent Relevant Breaches

HOW:

- One leaked folder exposed 91 sensitive databases.
- An update was needed to a tool they used internally for development purposes.
- Required all employees to complete and update to an internal program they use.
  - 0/170 employees completed the update.

WHAT:

- Names, addresses, phone numbers, email addresses, IP addresses, automobile details, VIN numbers, car service records, damage claims, hashed passwords, text and email messages with clients.

PURPOSE:

- Insurance scams, with criminals using personally identifiable information, damage claims, extended car details, and dealer and warranty information to target insurance companies and policyholders.
- Details can be used to break into other platforms such as bank accounts, personal email accounts, and corporate systems.

Breaches are going to happen…

…readiness is a choice!

TIMELINES

BEFORE

BREACH

AFTER

cieca

Collision Industry Electronic Commerce Association

BEFORE: Protecting “The Data” with Cybersecurity

Invest & Implement a Cybersecurity program company-wide.

- On-going awareness with all employees (culture).
- Incident response plan.

Figure out what framework you are going to use.

Implement solid product release processes.

Cyber Insurance.

- Do not hide behind cheap insurance policies.

Audit your plan, and record metrics.

…this is the next health and safety.

AFTER: Further-Protecting "The Data" with Cybersecurity

Speed of response?

Execution of incident response plan.

Mitigation efforts towards what was not mitigated before.

Communication plan.

Designated roles for communication execution.

That was a lot to take in, what should we be doing to ensure we protect our industry and ensure future sustainability?

Steps towards prevention.

Implement a Framework

NIST Cyber Security Framework

or

ISO 2700x

Designed and updated regularly to anticipate advances in technologies and future challenges.

Recommendations

The Why:

By law, data needs to be protected.

- Poor practices lead to lawsuits and potentially heavy fines.

Cybersecurity framework is not QA.

- This is a collective effort that requires segregated duties.

Technology organizations need proactive protective control.

- Vulnerability analysis that are completed in staging, not in production.
- CISO or Security Roles are identified, and those team members have final signoff.

It doesn’t matter about the size of your organization, steps and measures need to be put in place and enforced.

Recommendations

The CARE Standard for Cybersecurity

C	**Consistent:** Do your controls work the same way over time?
A	**Adequate:** Do you have satisfactory and acceptable controls in line with business need?
R	**Reasonable:** Do you have appropriate, fair, and moderate controls?
E	**Effective:** Do you test these controls, and through testing, does it produce desired results?

The real question…

How might we fulfil our corporate social responsibility as it relates to cybersecurity by making it fundamental in our respective business cultures resulting in a collaborative industry strength.

…security and data privacy will become like health and safety standards.

Remember, it’s not the technology that is the risk, it’s the people.

cieca
Collision Industry Electronic Commerce Association

Contact Us

✉ Brandon.laur@claimscorpinc.com

📱 905.517.7243

🏢 2820 King Street East,
Hamilton, ON L8G 1J5

🌐 www.cciglobaltechnologies.com