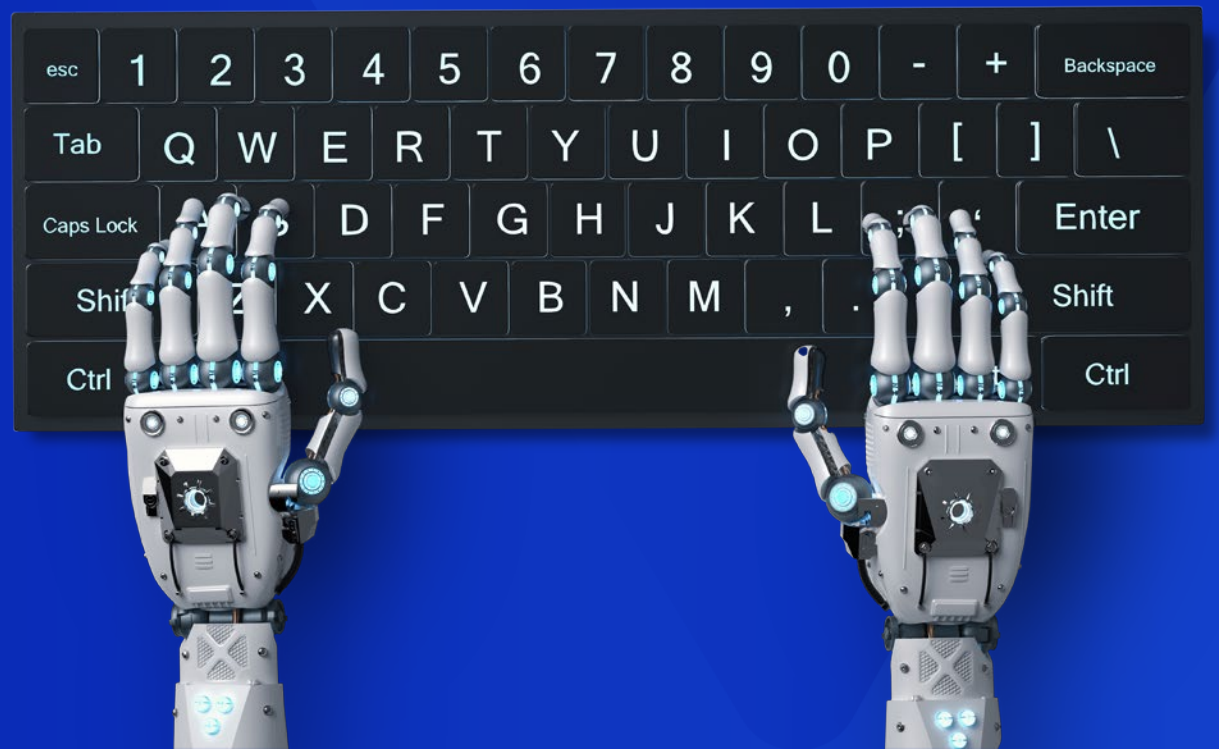
VICTOR | ProWriters
A VICTOR COMPANY

Cyber strategies for A&E

February 23, 2026



Your Hosts

Brandon Perry
A&E Large Firm Underwriting Leader

Zane Goldthorp
ProWriters Director of Broker Development

1. Who is ProWriters?
2. A&E Exposures
3. Claims examples
4. Digital IQ
5. Quote comparison
6. Cyber U
7. Q&A

Agenda

Who is ProWriters?

ProWriters benefits

Multiple quotes from top carriers in seconds

Revenues of all sizes — from startups to multi-million-dollar businesses.

Cyber U educational content/videos

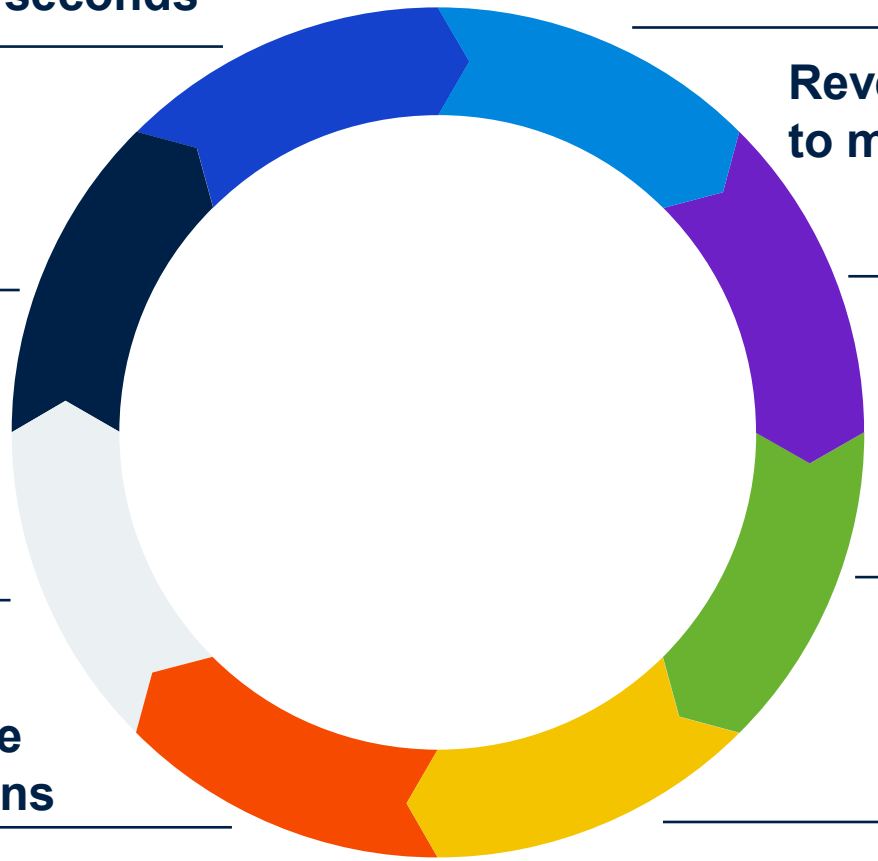
Personalized training and support for brokers/agents

Access to 60-plus cyber markets

Surplus lines licenses in every state

Competitive commissions

Admitted and non-admitted options



VICTOR | ProWriters A VICTOR COMPANY

A&E Exposures

1

Cyber Crime (Funds Transfer, Social Engineering, & Invoice Manipulation

A&E firms regularly:

- Send invoices
- Approve payment applications
- Exchange wiring instructions
- Coordinate with contractors, developers, and municipalities

Attackers impersonate executives, project managers, or vendors to:

- Redirect construction payments
- Change ACH instructions
- Divert escrow funds
- Losses often range from **$50K to $500K+** per incident.

VICTOR | ProWriters A VICTOR COMPANY

Ransomware Attacks

A&E firms rely heavily on:

- CAD files
- BIM models
- Project management platforms
- Cloud-based collaboration tools

Ransomware can:

- Lock project drawings and models
- Halt construction timelines
- Trigger contractual penalties
- Delay occupancy deadlines
- Because projects are time-sensitive, firms often feel pressure to pay.

Intellectual Property Theft

Design files contain:

- Proprietary architectural plans
- Structural engineering models
- Security layouts
- Infrastructure schematics

Stolen IP can:

- Be sold to competitors
- Be used in foreign development projects
- Create national security concerns (infrastructure, utilities, healthcare facilities)

Data Breach of Client & Employee Information

A&E firm's store:

- Employee SSNs & payroll data
- Client financial information
- Vendor W-9s
- Background check data
- Government project information

Exposure leads to:

- Notification costs
- Regulatory fines
- Credit monitoring expenses
- Reputational damage

Why A&E firms are targeted?

- They move large sums of money.
- They are central communication hubs for projects.
- They handle high-value intellectual property.
- Many mid-sized firms have limited internal IT security.
- Construction timelines create urgency attacker's exploit.

Common Cyber Claims Examples

Social engineering / invoice manipulation

The ACH-napping

Scenario

A large architecture firm received an email appearing to be from an MEP consultant requesting updated ACH information. The email chain was real – an attacker had infiltrated the consultant's Office365 account.

Impact

- $265,000 transferred to a fraudulent overseas account
- Vendor relationship strained

Takeaway

A&E firms frequently pay consultants, making them prime targets for funds-transfer fraud.

Ransomware

Lock, block & downtime shock!

Scenario

A mid-size architecture firm's file server was encrypted overnight. All CAD drawings, Revit models, and spec documents were locked.

Impact

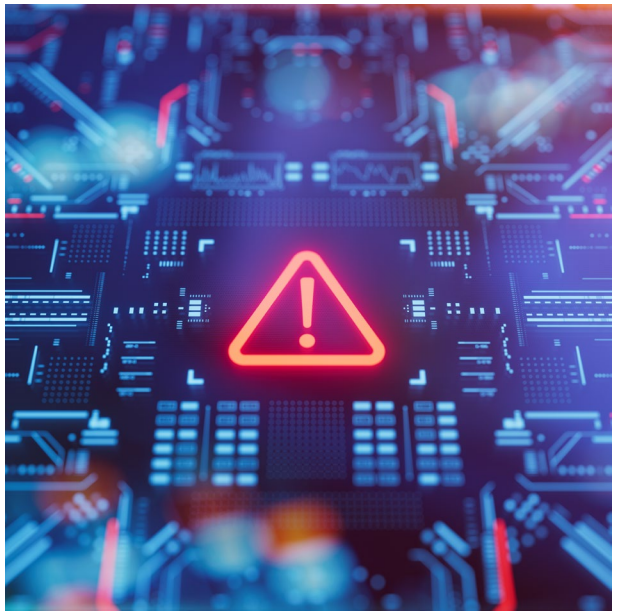
- 10 days of total downtime
- $175,000 in forensic and restoration costs
- $80,000 in lost productivity and missed deadlines
- Required IT rebuild because backups were also corrupted

Takeaway

A&E firms are prime ransomware targets because project files are high-value and time-sensitive.

Backup failure

Backup breakdown turns small virus incident into a major loss



Scenario

A minor malware incident spread into a backup system that had not been properly segmented.

Impact

- All active projects had to be restored manually
- 1,500 hours of rework
- $300,000+ total loss

Takeaway

Backup integrity is one of the largest determining factors in the severity of A&E cyber claims.

Digital IQ

ProWriters

- Product Selection
- Applicant Information
- Business Information
- Security and Controls
- Claims and Coverages

Applicant Information

Start typing company name and full address

Company ABC, 123 Main Street

Or enter below

Company Name

Street

Suite/Unit/Floor etc.

City

State

Select

Zip code

Website, URL, or Domain (enter all that apply)

The applicant does not have a website, URL, or domain.

Back

Next

ProWriters

- Product Selection
- Applicant Information
- **Business Information**
- Security and Controls
- Claims and Coverages

Business Information

Gross Revenue (Projected for the next 12 months)

$

Record Count (if you're not sure, leave it blank and we'll estimate for you)

Number of Employees (if you're not sure, leave it blank and we'll estimate for you)

NAICS Code / Industry Description (If you can't find the right code, search the NAICS database)

Begin typing your industry or related keywords to find your NAICS code

Back

Next

ProWriters

- Product Selection
- Applicant Information
- Business Information
- **Security and Controls**
- Claims and Coverages

Security and Controls

☐ I don't know the answers to any of these questions

Multi-factored Authentication (MFA)

Does the applicant have MFA in place for remote network access?

Yes	No	Uncertain

Does the applicant have MFA in place for email access?

Yes	No	Uncertain

Does the applicant have MFA in place for network administrators and other privileged users?

Yes	No	Uncertain

Back

Next

ProWriters

Product Selection
Applicant Information
Business Information
Security and Controls
Claims and Coverages

Security and Controls

☐ I don't know the answers to any of these questions

Endpoint Detection and Response (EDR)

Does the applicant use an EDR tool that includes centralized monitoring?

Yes	No	Uncertain

Backups

Does the applicant regularly back up and segregate sensitive data?

Yes	No	Uncertain

Email

Does the applicant use an email security filtering tool?

Yes	No	Uncertain

Back

Next

ProWriters

- Product Selection
- Applicant Information
- Business Information
- Security and Controls
- Claims and Coverages

Claims Information and Requested Coverage

Claims

Has the applicant had a claim or any knowledge of a circumstance that could lead to a claim within the past 5 years?

Yes | No

Limit Request

$1,000,000

Effective Date (Optional)

Quotes received may expire before the requested effective date and may need to be refreshed.

Additional Information (Optional)

Is there anything else we need to know? Add comments or upload files below.

Drag and Drop Files Here or Browse for Files

Back

Next

Gross Revenue
$5,000,000
Record Count
15,000 (estimate)
Number of Employees
25 (estimate)
Industry / NAICS code
541310 - Architectural Services
Policy Limit
$1,000,000
Requested Effective Date
Unknown

Create New Option

Get an EPL Quote

Quote ID
47849
Product
Cyber
Stage
Quoted
Status

	cfc	Coalition	elpha secure	at bay	beazley	TRAVELERS	TOKIO MARINE HCC	Westchester A Chubb Company	cowbell
	Admitted	Admitted	Non-Admitted	Non-Admitted	Admitted	Admitted	Non-Admitted	Admitted	Non-Admitted
Limit	$1,000,000	$1,000,000	$1,000,000	$1,000,000	$1,000,000	$1,000,000	$1,000,000	$1,000,000	$1,000,000
Retention	$5,000	$5,000	$2,500	$5,000	$1,000	$5,000			
Premium	$1,860	$3,878	$1,920	$3,308	$2,400	$6,336	Referral	Referral	Referral
Applications	Application	Application	Application	Application	Application	Application	Application	Application	Application
Documents									
Compare									
Bind									

Request Bind

Broker contact information
Colin Quinn
484-320-2088
colin.quinn@prowritersins.com

Coverage & Quote Comparison

4

ProWriters

Professional & Management Liability Insurance

Quote ID:	47849
Revenue:	$5,000,000
Record count:	15,000
Date:	2/18/2026

	cfc	Coalition	elpha secure	at bay	beazley	TRAVELERS
Admitted vs. Non-Admitted	Admitted	Admitted	Non-Admitted	Non-Admitted	Admitted	Admitted
Rating / Size	A / IX	A- / VII	A / XV	A- / VII	A / XV	A++ / XV
Prior Acts	Full Prior Acts	Full Prior Acts	Full Prior Acts	Full Prior Acts	Full Prior Acts	Full Prior Acts
Limit	$1,000,000	$1,000,000	$1,000,000	$1,000,000	$1,000,000	$1,000,000
Deductible / SIR	$5,000	$5,000	$2,500	$5,000	$1,000	$5,000
Premium	$1,860.00	$3,878.00	$1,920.00	$3,308.00	$2,400.00	$6,336.00
Taxes and Fees	$0.00	$0.00	$180.80	$361.12	$0.00	$0.00
Total Payable	**$1,860.00**	**$3,878.00**	**$2,100.80**	**$3,669.12**	**$2,400.00**	**$6,336.00**

	cfc	Coalition	elpha secure	at bay	beazley	TRAVELERS
1st Party Liability						
Breach Response & Remediation	$1M	$1M	$1M	$1M	$1M	$1M
Cyber Business Interruption (BI)	$1M	$1M	$1M	$1M	$1M	$1M
Dependent BI – IT	$1M	$1M	$1M	$1M	$1M	$1M
Dependent BI – Non-IT	-	-	-	$1M	$1M	$1M
System Failure	$1M	$1M	$1M	$1M	$1M	$1M
Dependent System Failure – IT	$1M	$1M	$1M	$1M	$1M	$1M
Dependent System Failure – Non-IT	-	-	-	$1M	$1M	$1M
BI Waiting Period	8 hrs	8 hrs	8 hrs	8 hrs	8 hrs	8 hrs
Dependent BI Waiting Period	8 hrs	8 hrs	8 hrs	8 hrs	8 hrs	8 hrs
Ransomware / Cyber Extortion	$1M	$1M	$1M	$1M	$1M	$1M
Ransomware Payment Provision	Reimbursement	Pay on behalf	Reimbursement	Pay on behalf	Reimbursement	Reimbursement
Digital Asset Damage	$1M	$1M	$1M	$1M	$1M	$1M
Cyber Crime	$100K / $5K	$250K / $5K	$250K / $2.5K	$250K / $5K	$250K / $1K	$1M / $2.5K
Social Engineering	$100K / $5K	$250K / $5K	$250K / $2.5K	$250K / $5K	$250K / $1K	$250K / $2.5K
Client Funds	$100K / $5K	$250K / $5K	$250K / $2.5K	$250K / $5K	-	-
Invoice Manipulation	$50K / $5K	$250K / $5K	$250K / $2.5K	$250K / $5K	$250K / $1K	$250K / $2.5K
Telephone Hacking	$100K / $5K	$250K / $5K	$250K / $2.5K	$1M / $5K	$250K / $1K	$250K / $2.5K
Crypto Jacking	$100K / $5K	$250K / $5K	$250K / $2.5K	$1M / $5K	$1M / $1K	-
Reputational Harm	$1M	$1M	$1M	$1M	$1M	$1M
Breach Response (Outside the Limit)	$1M	$1M	$1M	$1M	$1M	-
Bricking	$1M	$1M	$1M	$1M	$1M	$1M
Bodily Injury	-	$250K	-	-	-	-
Property Damage	-	$250K	-	-	-	-
BYOD	Yes	Yes	Yes	Yes	Yes	Yes

Coverage Descriptions

1st Party Liability	Description
Breach Response & Remediation	Coverage for response and remediation costs associated with a breach; This includes legal fees, customer notification, IT/digital forensics, and crisis media relations, among others.
Cyber Business Interruption (BI)	Coverage for financial losses due to a cyber event that causes degradation to your computer system; Usually requires a time retention (see Business Interruption Waiting Period).
Dependent BI – IT	Coverage for financial losses due to a cyber event when a 3rd party provider experiences a cyber event that causes you disruption; 3rd parties often include cloud providers or other software/services/hosting providers.
Dependent BI – Non-IT	Coverage for financial losses due to a cyber event when a 3rd party provider experiences a cyber event that causes you disruption; 3rd parties often include Non-IT entities providing necessary products or services to the insured.
System Failure	Coverage for financial losses due to business interruption resulting from an unplanned or unintentional outage, often caused by employee error or power outage.
Dependent System Failure – IT	Coverage for financial losses due to business interruption resulting from an unplanned or unintentional outage of a system operated by a 3rd party vendor providing cloud/software/hosting services, often caused by employee error or power outage.
Dependent System Failure – Non-IT	Coverage for financial losses due to business interruption resulting from an unplanned or unintentional outage of a system operated by a 3rd party Non-IT vendor providing necessary products or services, often caused by employee error or power outage.
BI Waiting Period	Time retention typically applied to cyber business interruption and system failure.
Dependent BI Waiting Period	Time retention typically applied to cyber dependent business interruption and dependent system failure.
Ransomware / Cyber Extortion	Coverage for the costs to respond to a cyber extortion (ransomware) event, including forensics experts to investigate the attack, experienced negotiators, and sometimes ransom payments in virtual currencies.
Ransomware Payment Provision	Provision for how the policy responds to a ransomware claim; "Pay on behalf" indicates the carrier will tender payments due when a ransom event occurs; "Reimbursement" indicates the insured will pay out of pocket and then seek reimbursement for covered lo
Digital Asset Damage	Coverage for costs to rebuild electronic data and other digital assets after a cyber-event, like recovering offsite backups, etc.
Cyber Crime	Coverage for the theft of funds from a failure in your security, often by a hacker stealing login credentials; This is often referred to as fund transfer fraud and may be covered on a crime policy.
Social Engineering	Coverage for theft of funds via deception or impersonation where a criminal tricks you into parting with your funds; often linked to business email compromise
Client Funds	Coverage extension to cover theft of client funds in the insured's care, custody, or control.
Invoice Manipulation	Coverage for the release or distribution of a fraudulent invoice or fraudulent payment instruction to a third party as a result of a cyber-event.
Telephone Hacking	Coverage for costs associated with unauthorized and fraudulent telephone calls.
Crypto Jacking	Coverage for costs associated with unauthorized use of the insured's computer processing power to mine crypto currency.
Reputational Harm	Coverage for lost income from an adverse media event due to a cyber event that damages the insured's reputation.
Breach Response (Outside the Limit)	Coverage for 1st party breach costs outside of and in addition to the policy aggregate limit.

Cyber U

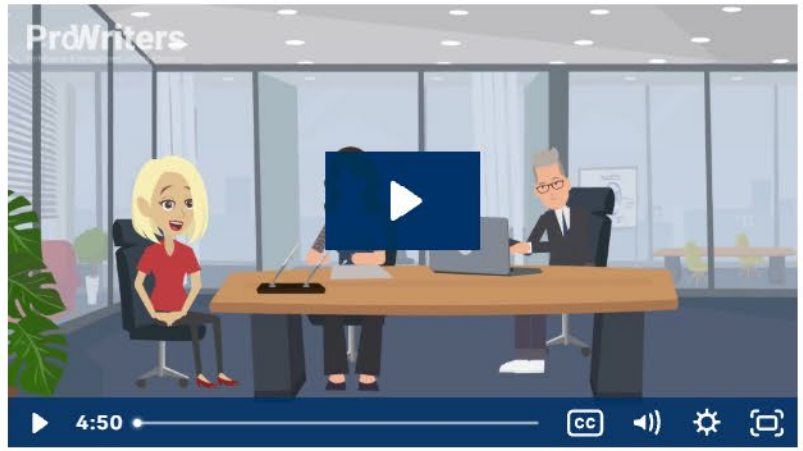
Welcome to Cyber U

Educate yourself and your clients on Cyber Insurance and cyber threats with Cyber U! This comprehensive online resource delivers bite-sized video lessons demystifying the world of cyber insurance.

Whether you're a seasoned cyber agent or simply curious about protecting your digital assets, Cyber U equips you with the knowledge and confidence to navigate this ever-evolving landscape. Share these informative videos with colleagues and clients by right clicking on the video and selecting "Copy link and thumbnail". So, click, learn, and stay ahead of the curve – Cyber U is your passport to cyber awareness!

Cyber on the BOP...Agent's Worst Nightmare

Cyber Endorsement on your BOP does not always mean your business is protected. In the event on a cyber breach, learn just how important it is to ensure you're fully covered.



What to do in the Event of A Cyber Claim

What should you do if your clients have had a breach? ProWriters covers one of their most common questions.

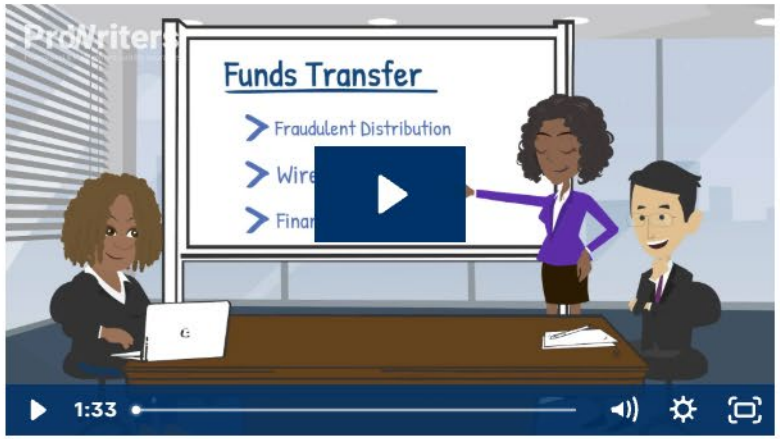
History of Cyber Crime

In the event of a cyber crime, should cyber or crime policy respond? Both! Learn how the histroy of cyber insurance came to be.

+ **Industry Specific**
+ **Ransomware**
+ **Cyber Crime**
+ **1st Party Cyber Coverages**
+ **Cyber Preventative Tools**

− Cyber Crime

History of Cyber Crime



Funds Transfer

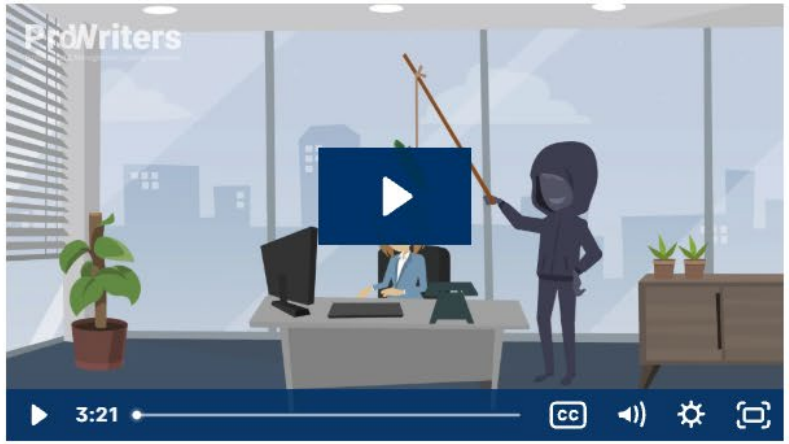
Social Engineering

Invoice Manipulation

Loss of Tangible Property

Social Engineering Prevention

− Industry Specific



Why ALL Businesses need Cyber

Cyber for A&E Firms

Cyber for Auto Dealerships

Why Financial Services Firms Need Cyber

Cyber for Real Estate Firms

Why Contractors Need Cyber

Q&A

Thank you

VICTOR

This document is for illustrative purposes only and is not a contract. It is intended to provide a general overview of the program described. Please remember only the insurance policy can give actual terms, coverage, amounts, conditions and exclusions. Program availability and coverage are subject to individual underwriting criteria.

Victor Insurance Services LLC in MN | DBA in CA and NY: Victor Insurance Services | CA Ins. Lic. # 0156109