Private conversations are taking place in public spaces

And they can be heard and read by Internet service providers,
state-enabled hackers engaged in industrial espionage, and others.

CFO: Our quarterly earnings beat our earlier guidance by 4%

CEO: The board and market will be thrilled to hear that!

CFO: Time to consider buying ACME... They're stock is tanking and they're assets are worth 10x the ask

CEO: Keep it under wraps until they drop below $16 per share, and buy in small blocks using various brokers up and until $20

Board Member: The board is thinking about firing Joe... he's a liability and they want to cut their losses

CEO: I'll let him know, I don't want him blindsided. No need to alienate him. He could take his knowledge to our competitor and make our lives harder than need be

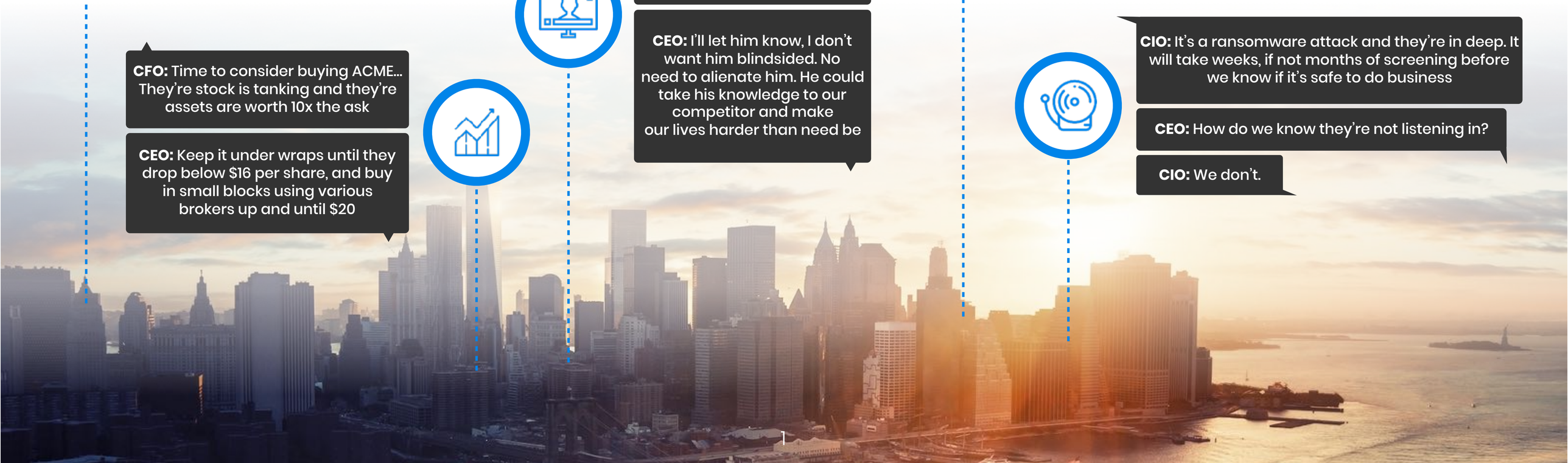
GC: We've got a lot of exposure and we should look to settle with them while they're still open to negotiations

COO: Let's keep this quiet. I'm on the hook and the board is going to want a blood sacrifice

CIO: It's a ransomware attack and they're in deep. It will take weeks, if not months of screening before we know if it's safe to do business

CEO: How do we know they're not listening in?

CIO: We don't.



ARMORTEXT

Your business conversations, videos, and files encrypted end-to-end

Available on any major desktop or mobile device

Built for Defense & Government Advisory Services, Energy & Utilities, Legal, Healthcare, and Financial Services

With Enterprise Governance, Data Retention & Review, and Information Lifecycle Controls

Capabilities	ARMORTEXT
True End-to-End Encryption (For Client-Eyes-Only)	✓
Secure Messaging & Fileshare (Any OS, Device, Tablet & Desktop)	✓
Secure 1-on-1 & Group Messaging	✓
Enterprise Controls	✓
Information Lifecycle Controls	✓
Compartmented Communications & Risk Reduction Strategy	✓
Admin w/o Read Access (No Snowden Effect)	✓
Cryptographically Enforced Scopes of Review	✓
No Proprietary Hardware or Infrastructure Requirements	✓
Encrypted Voice	**Q2 2018** - In Beta
Encrypted Video Conferencing	**Q3 2018** - In Beta
Archive Integrity Verification	**Q4 2018** - In Beta

- **We can't decrypt or read customer data**
- **Available on iOS, Android, PC, Mac, and Linux**
- ArmorText is a hyper-evolution in secure enterprise messaging. Our competitors lack risk reduction strategies such as compartmented communications, segregation of duties, and cryptographically enforced scopes of review
- **Guards against unintended disclosures** (plain view doctrine)
- **Patent Pending**

These organizations employed the wrong solutions and put their companies, reputations, and profits at risk

$770M failed electoral bid
due to embarrassing leaks
Leaks undermined the credibility, intent and trustworthiness of the candidate, the DNC, and the political process.

$1M+ for insider trading case
due to a rogue IT admin
Example of insider threat, and board and c-suite vulnerability. An IT admin read c-suite comms prior to earnings calls to time trades on the exchange

Energy provider left vulnerable
due to communications shutdown
When hit by a crippling ransomware attack, BWL had no secure redundant communications capability in place to coordinate an emergency response

With ArmorText they would have been secure & better prepared...

Hyper-Secure Collaboration

True end-to-end encryption, unique ciphers for every message and attachment, and multi-factor authentication render phished passwords useless, and make bulk-hacks impossible

No Snowden Effect

It admins can manage ArmorText without being able to decrypt and read user conversations and attachments

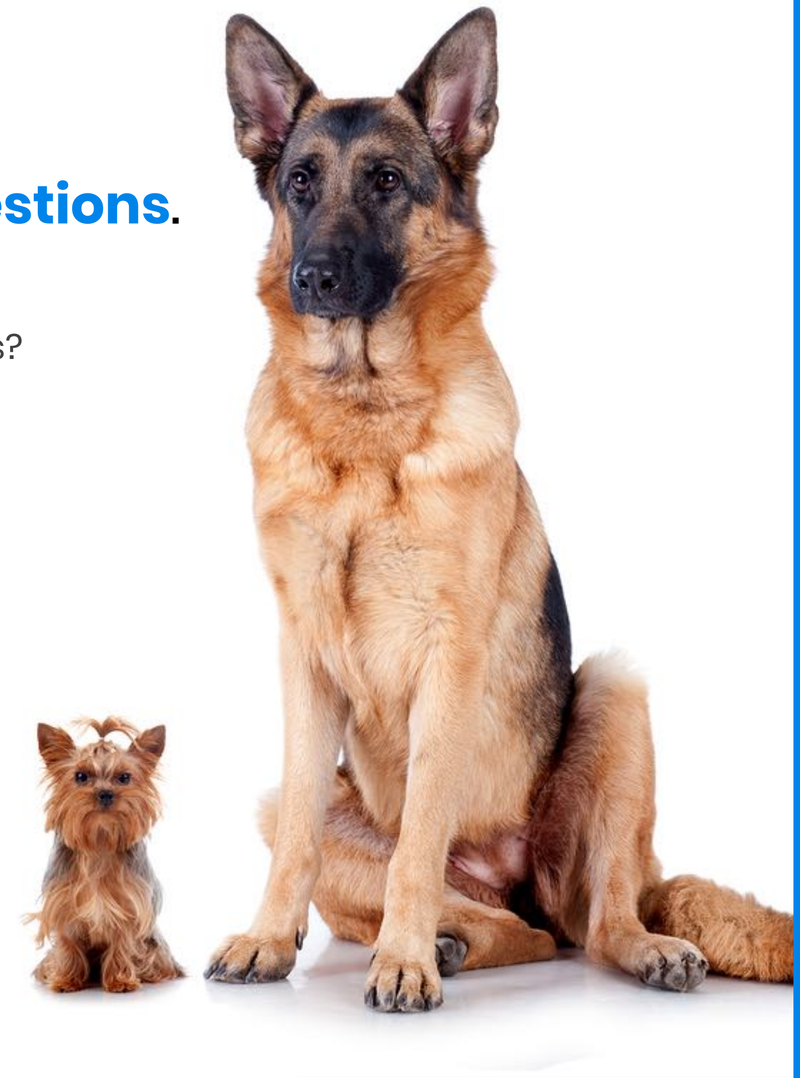
Crisis Management Communications

ArmorText is a cloud-based SaaS solution that provides a secure and redundant channel for communicating when your network is compromised

There are messengers and there's ArmorText...
AND THEY'RE NOT EQUAL OR ALIKE.

To tell the difference, all you have to do is ask the **right questions**.

1. Does our messenger use strong-encryption and is it truly end-to-end?
2. Can our internet service providers and others decrypt and read our data in their servers?
3. Does it provide enterprise controls?
4. Does it have information lifecycle controls?
5. Does it compartmentalize communications to defend against "plain view doctrine?"
6. Is it easy to use and deploy across the enterprise?
7. Is it an app and cloud based SaaS solution, or does it require expensive infrastructure or proprietary hardware?
8. Does it work across OS's, and with all mobile devices, tablets, and desktops?
9. Does it work in faraway and remote places around the world?
10. Is it a unified offering (message, file share, voice & video)?
11. Can we verify the integrity of any archives they hold on our behalf?
12. Do they provide technical support and consultation to help improve communications security?



Want to know what your CIO, CTO, CISO, and GC should be asking when they assess collaboration solutions for your organization?

READ:

"Eight factors C-Suites, CIO's, CISO's, Compliance Officers and your General Counsel should consider when evaluating and selecting a secure enterprise messenger/collaboration tool"

and

"Messaging Security, Governance, & User Experience Checklist"

ARMORTEXT

https://www.armortext.com