MAXXSURE
CYBER RISK MANAGEMENT

5 Threats

to Business Revenue Streams

A Ransomware Attack Could Shut Down Your Entire Business

Ransomware locks your systems, freezes operations, and blocks access to critical data. Your team can't process orders, communicate with customers, or access financial systems. Production stops. Revenue disappears. The average ransomware recovery takes 21 days.
Could your business survive three weeks without revenue while you rebuild systems?

AI Can Clone Your Executives' Voices to Authorize Fraudulent Transfers

New AI technology can perfectly replicate your CEO's or CFO's voice using just 3 seconds of audio from a conference call or video. Attackers call your finance team with a flawless voice clone and authorize a multi-million dollar wire transfer. By the time you discover it's fraud, the money is gone. Traditional verification processes can't detect these AI-powered impersonations.
Could your finance team detect a perfect AI impersonation of your CEO?

A Data Breach Could Destroy Customer Trust and Your Reputation

Hackers steal customer data, payment information, or confidential business records. News spreads immediately. Customers lose trust and take their business elsewhere. Your brand reputation, built over years, collapses in days. Class action lawsuits follow. Regulatory fines pile up. Credit monitoring costs add up quickly. Long-term revenue loss from customer defection often exceeds the average cost of a data breach
How would your business recover if your customers stopped trusting you?

Your Vendors and Partners Could Be Your Weakest Link

You trust your cloud provider, payment processor, software vendors, and IT partners. But hackers attack them first, then use their access to infiltrate your systems. 62% of breaches originate from third parties. Your security doesn't matter if your vendors have weak controls. When they get breached, you get breached...and your insurance may not cover it.
Do you actually know how secure your critical vendors are?

Your Cyber Insurance Could Disappear Right When You Need It

Insurance companies are getting stricter every year. At renewal, they audit your cybersecurity controls. If they find gaps, they either refuse to renew, triple your premiums, or slash your coverage limits. Then a major attack happens and you're facing millions in losses with inadequate or no insurance. 80% of organizations hit by cyber incidents discover they're underinsured only after the damage is done.
Would your current insurance actually cover a major breach?

How Maxxsure Helps

- **Financial Exposure Analysis**
- **Simple, Executive-Level Cyber Risk Scoring**
- **Cyber Insurance Alignment**
- **Analytics That Drive Action**
- **Ongoing Risk Monitoring**

Ready to Protect Your Gaming Enterprise with Maxxsure?

Email **nancy.viner@maxxsure.com** to schedule a 20-min call