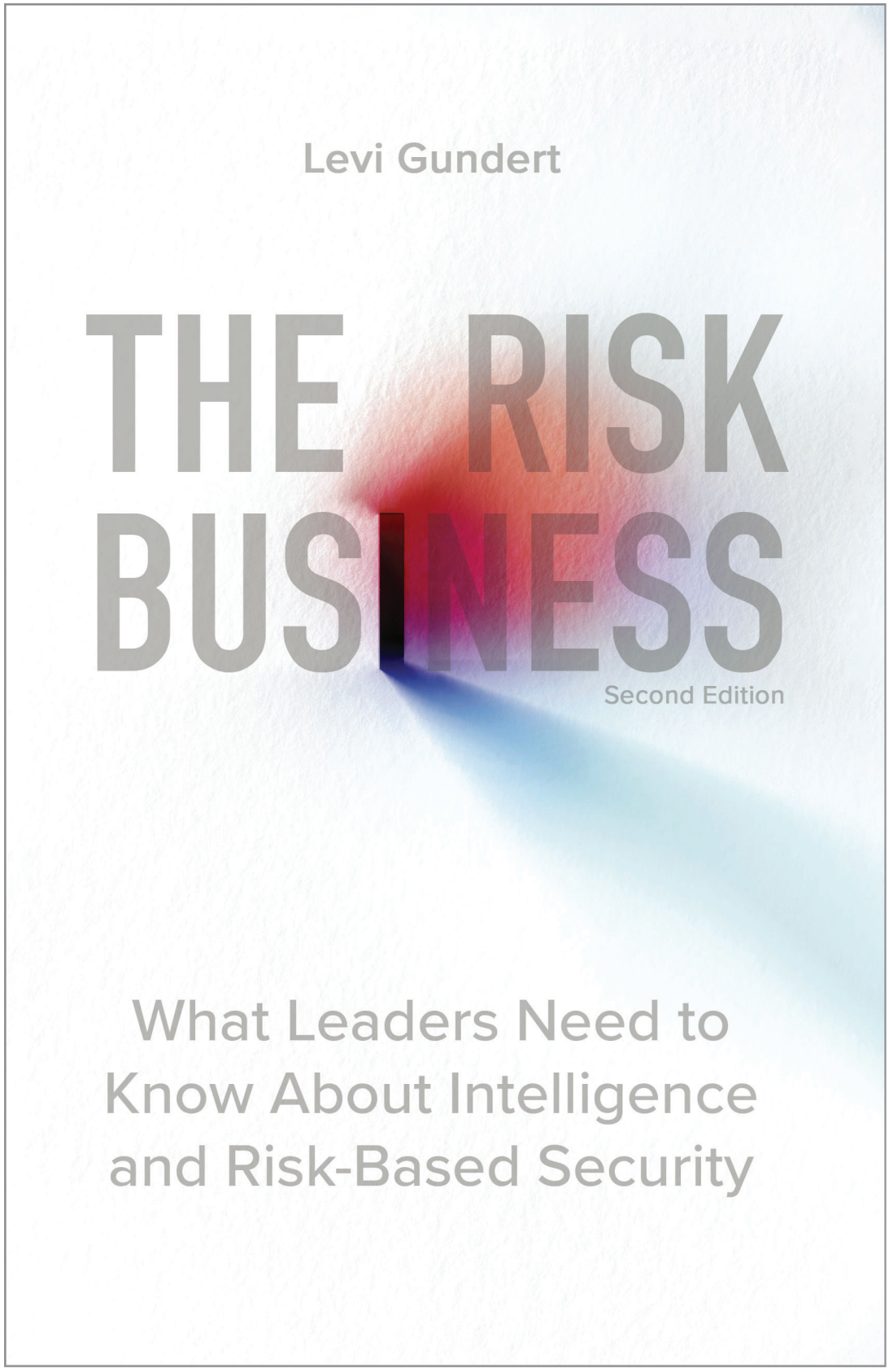
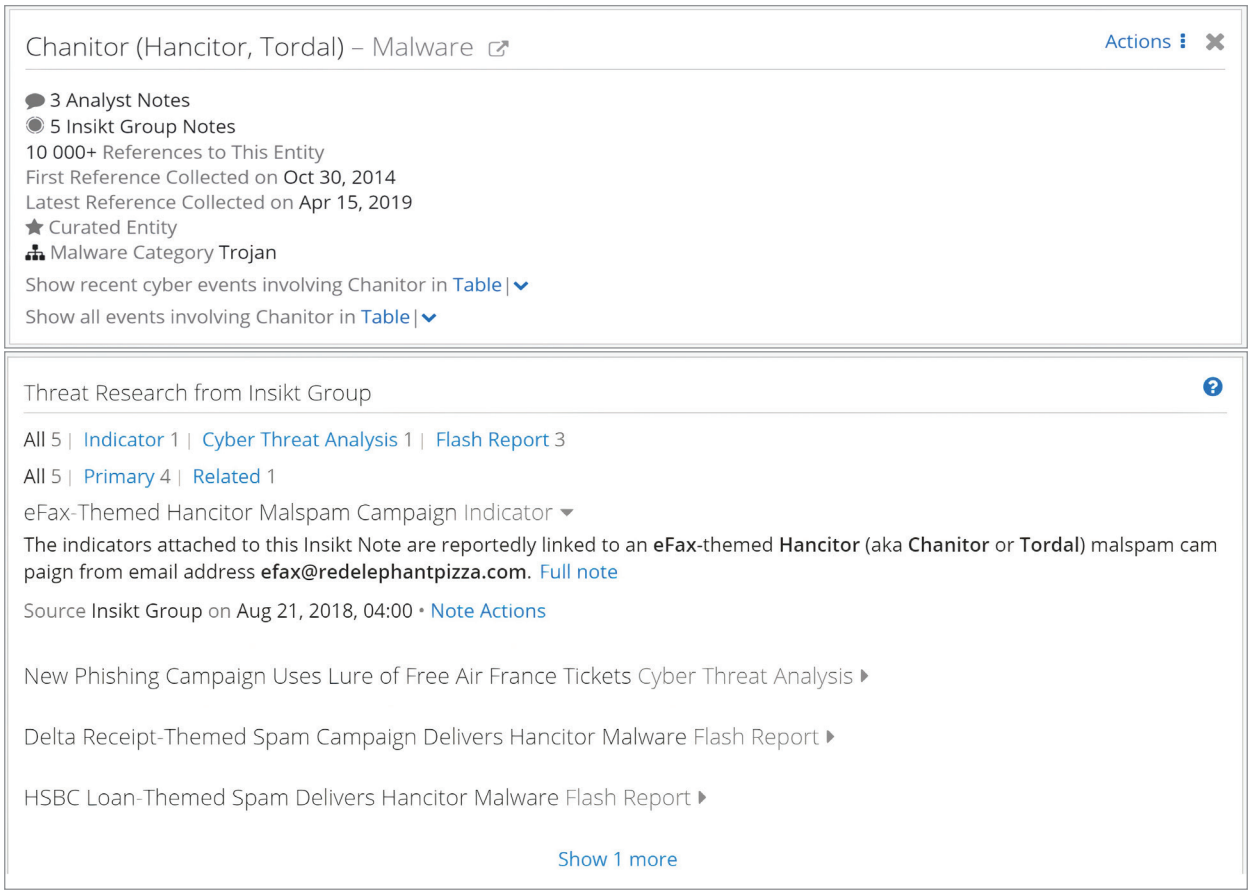
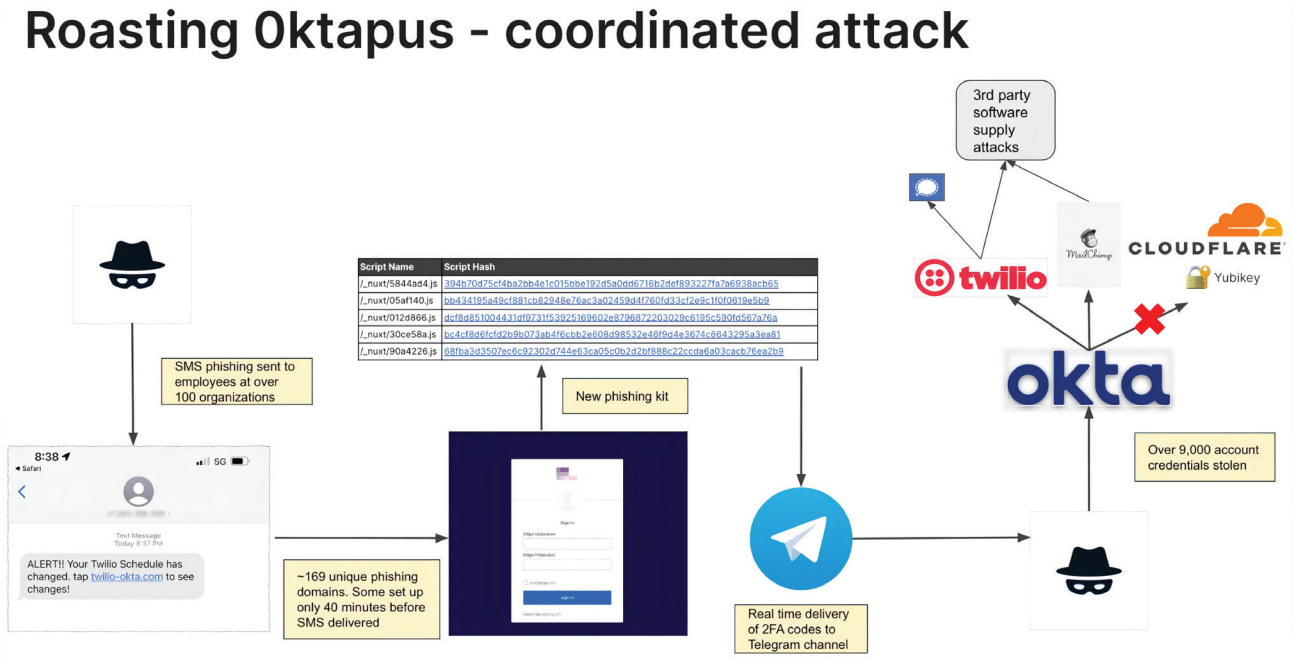
FIGURE SUPPLEMENT

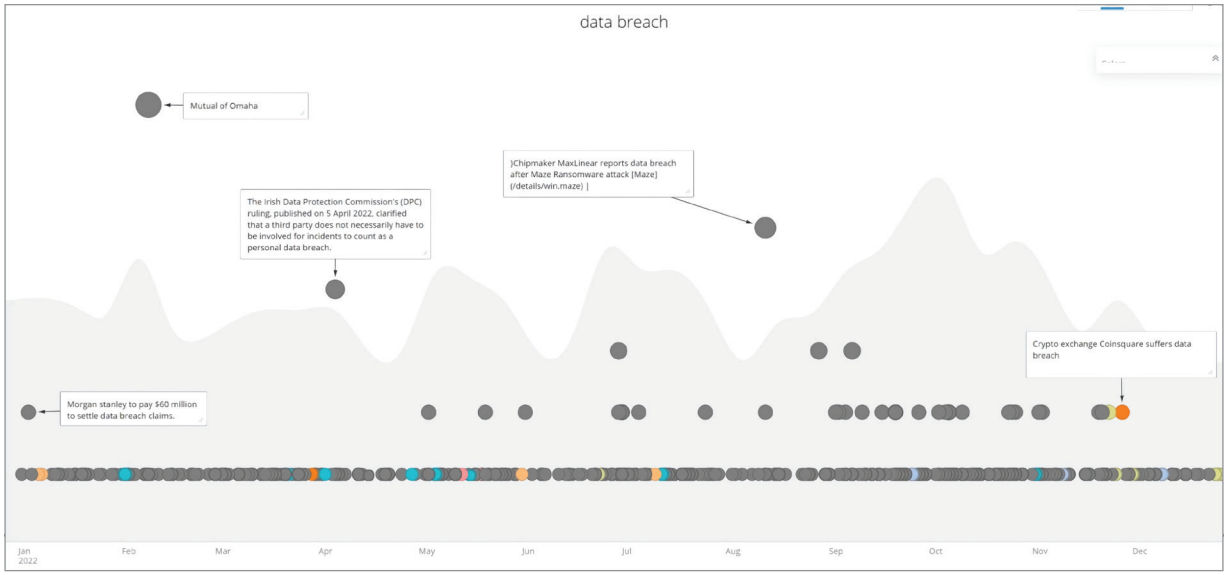




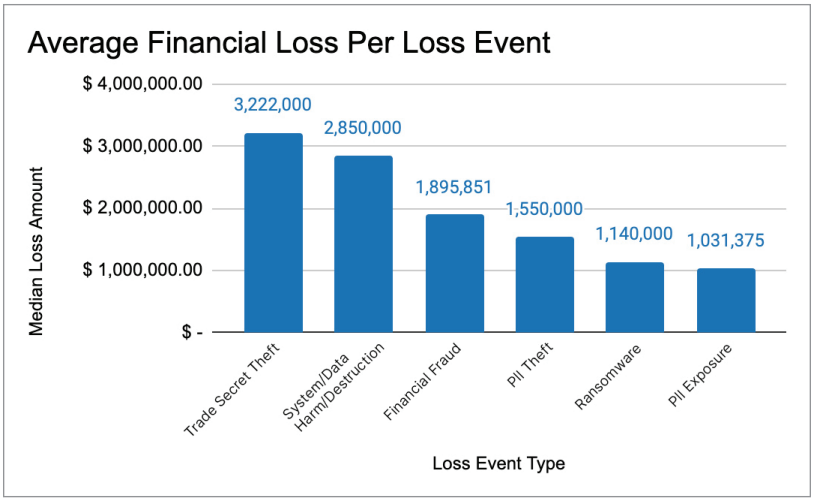
Recorded Future Intelligence Card for Hancitor/Chanitor (snapshot taken on April 15, 2019)



Flow of the Roasting Oktapus coordinated attack (Source: Recorded Future)



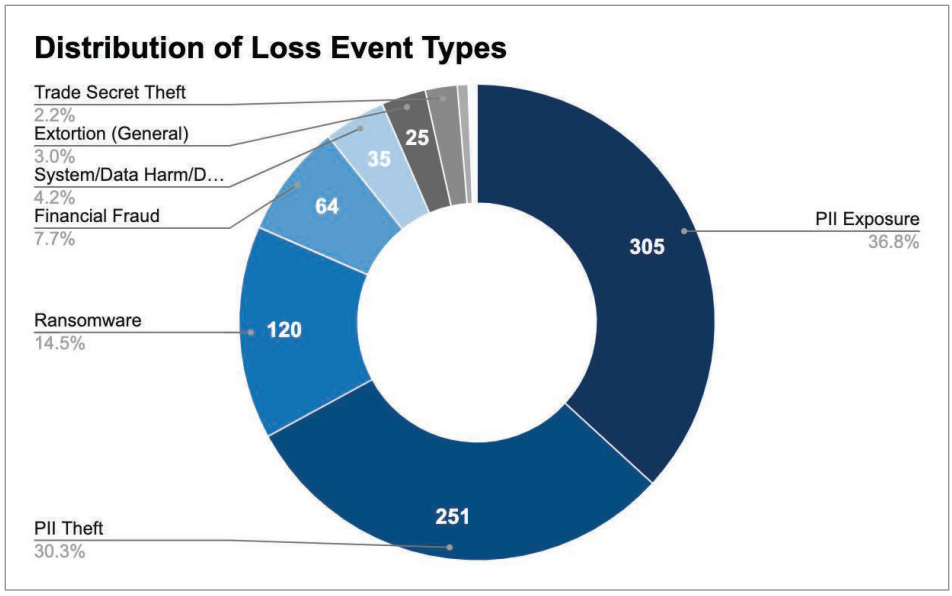
Timeline of data breaches in 2022, showing some of the more than 400,000 results (Source: Recorded Future)



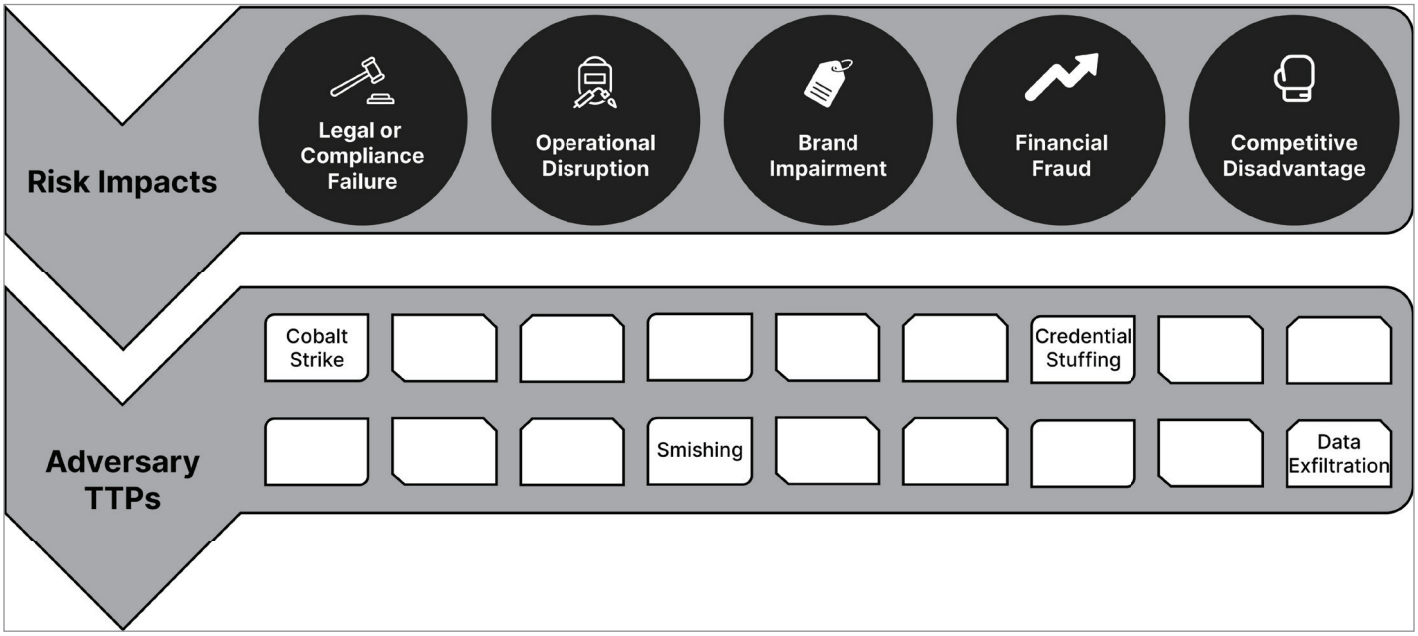
Median financial loss per event, by loss type (Source: Recorded Future)

Industry	Median of Loss Amount ($)	Count of Industry
Industrials	$15,200,000	22
Energy	$10,600,000	5
Consumer Staples	$4,662,500	17
Information Technology	$4,625,000	54
Finance	$2,750,000	63
Government	$2,700,000	3
Real Estate	$1,500,000	2
Consumer Discretionary	$1,339,481	41
Healthcare	$1,020,000	117
Services	$457,059	74
Communication Services	$300,000	15

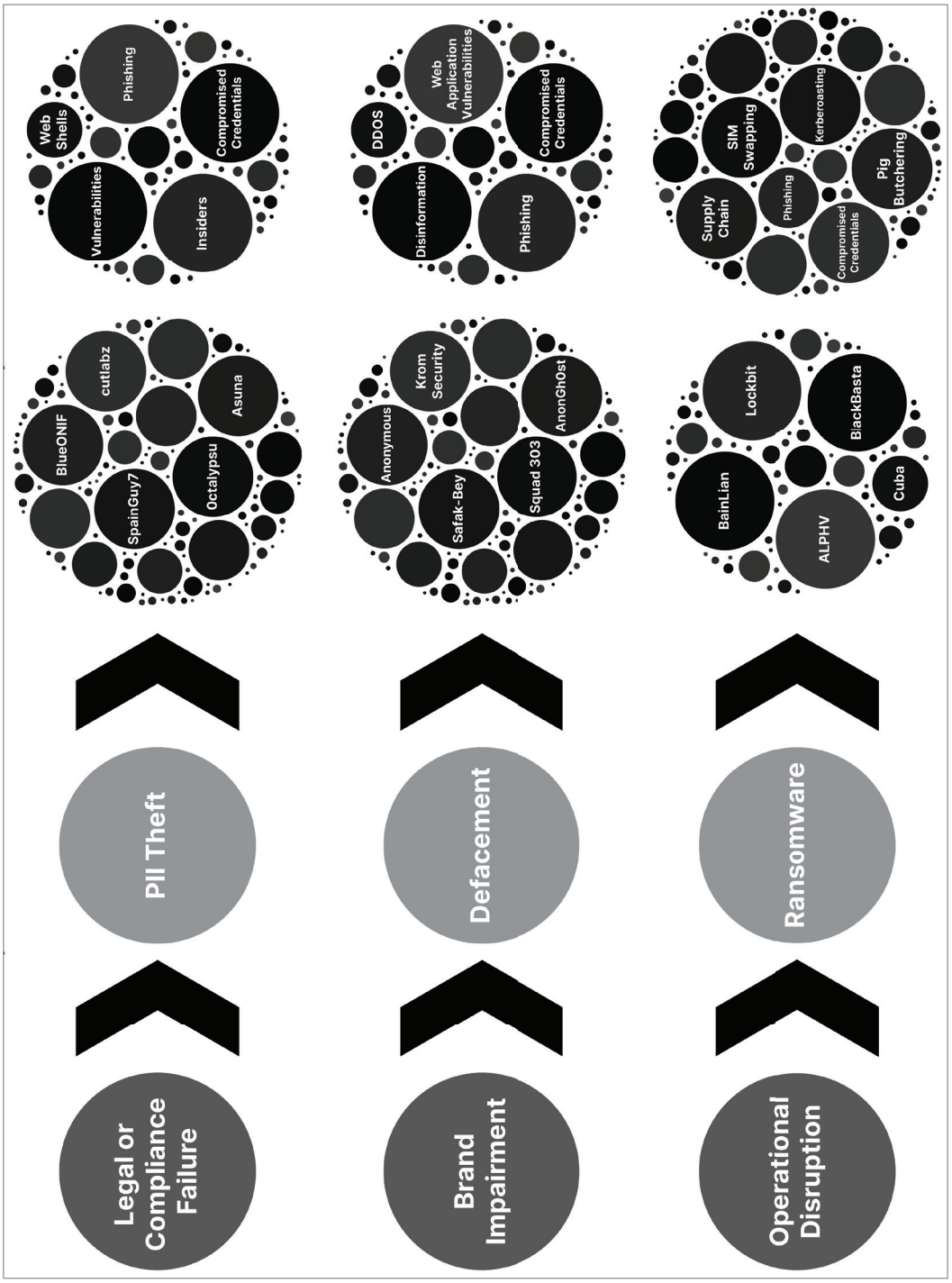
Median financial loss per event, by industry (Source: Recorded Future)



Percentage of loss events, by risk category (Source: Recorded Future)

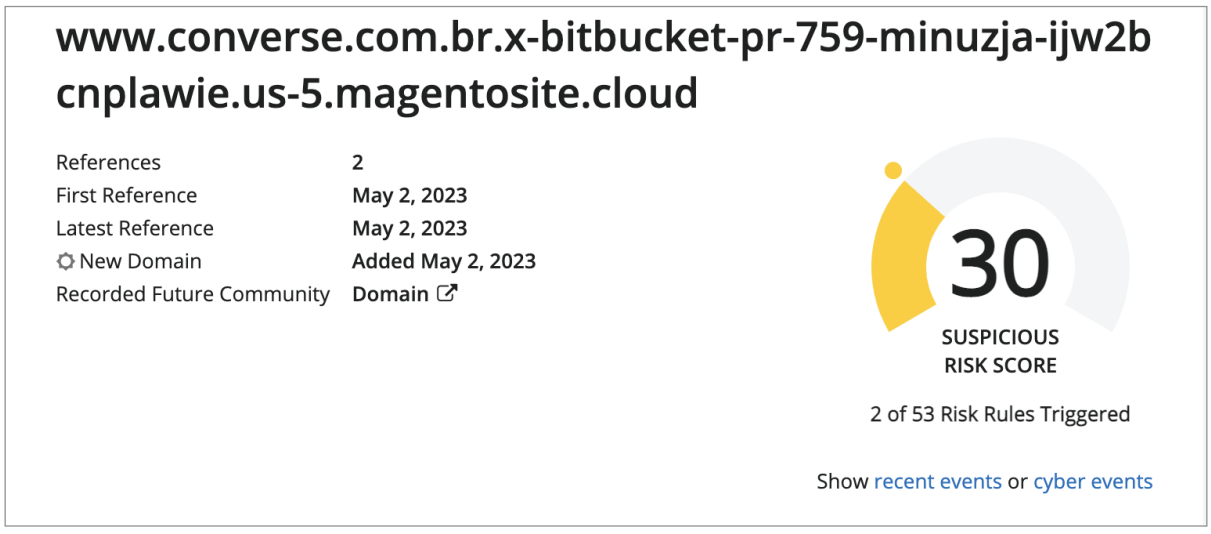


A security team worried about a particular risk impact can work backward to the related TTPs

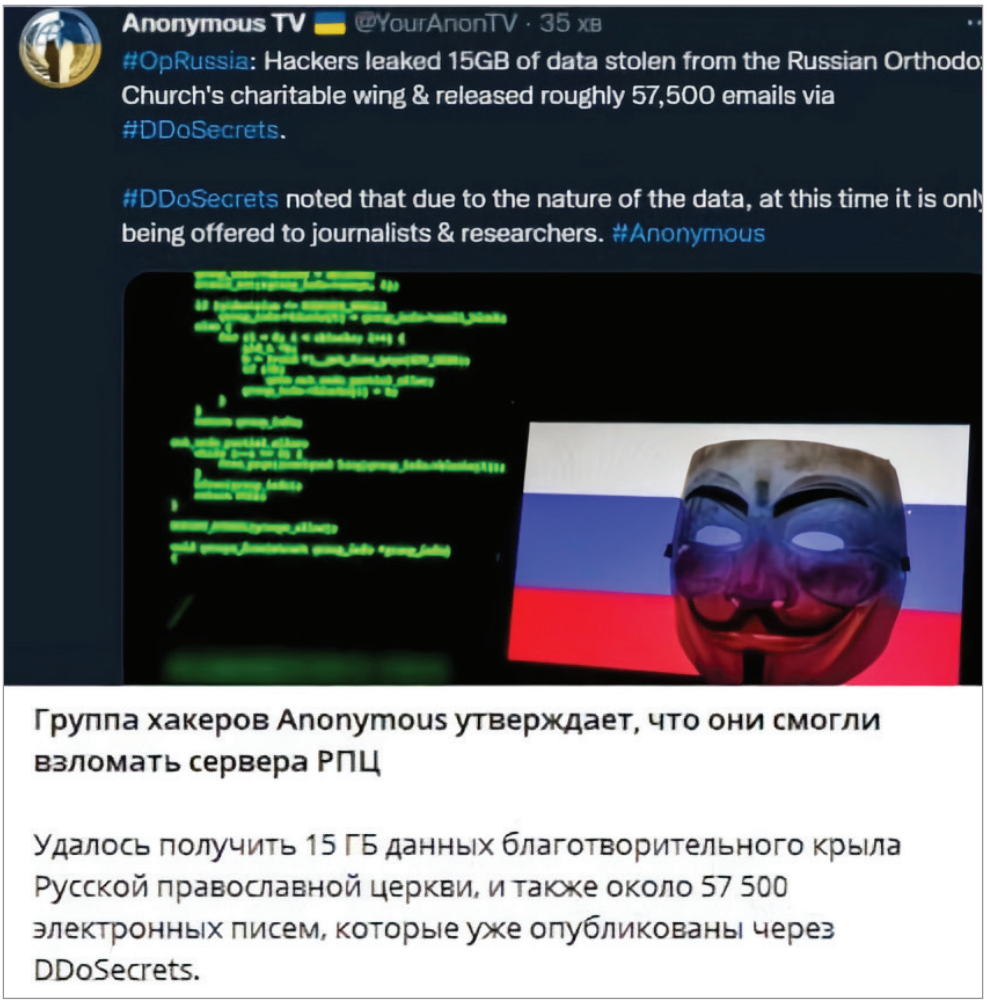


Nina and her team pinpointed the most important threat actors and their TTPs based on attack types with the highest potential impact on ACME and the greatest proximity (occurrence at similar organizations)

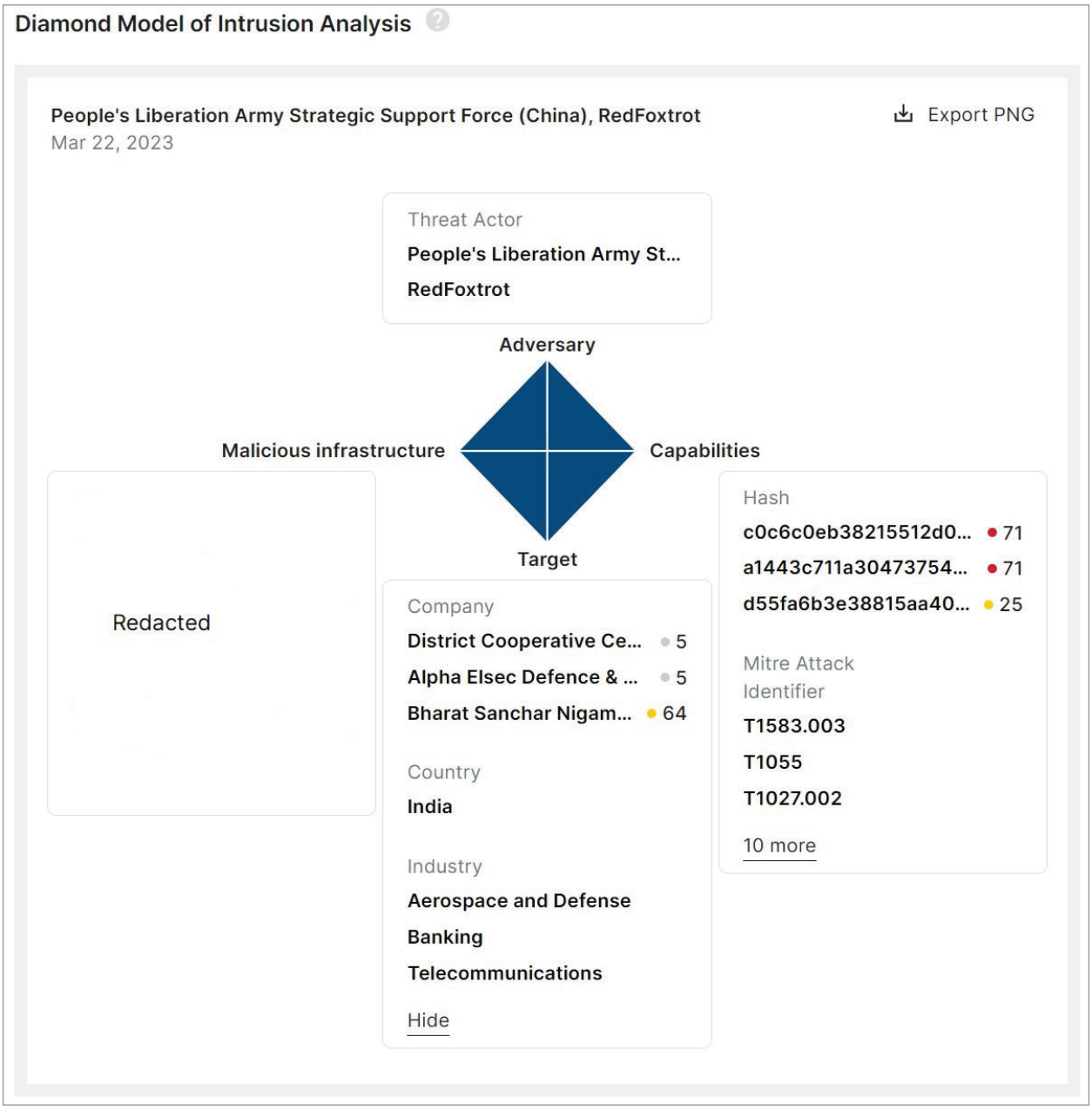
Ransomware extortion websites like Vice Society impair brand image by increasing the visibility of successful data breaches



An example of a typosquatted domain, in this case spoofing Converse[.]com, shown in a Recorded Future Intelligence Card



An example of hacktivists publishing stolen information from a religious organization.



An example of the Diamond Model of Intrusion Analysis in the Recorded Future Intelligence Cloud. It outlines the malicious infrastructure and techniques that RedFoxtrot, a Chinese state-sponsored threat activity group, used to attack Indian organizations in various industries in the first quarter of 2023.

Initial Compromise (Left of Boom)	Post-Compromise (Right of Boom)
Social Engineering*	Denial of Service (DoS)
Credential or Key Reuse/ Stuffing/Brute Forcing	Theft of Employee or Customer Personally Identifiable Information (PII)
Misusing Open Ports/ Network Shares (Manual or Automated — Worms)	Theft of Proprietary Communications or Information
Web Application Vulnerabilities (Including Web Shells)	Access and Theft of Data from Connected Third Parties
Hardware Vulnerabilities	Blackmail/Extortion
Software Vulnerabilities	Destruction of Data or Systems Availability
Protocol Hijacking (BGP/DNS)	Removal of Confidence in Data Integrity
Physical Tampering	Financial Fraud

*Includes phishing, spear phishing, business email compromise, and mislabeling malicious files in P2P networks

Risk Type	Event Risk	CI Only	AV Only	Both
Credential Reuse	100%	60%	30%	10%

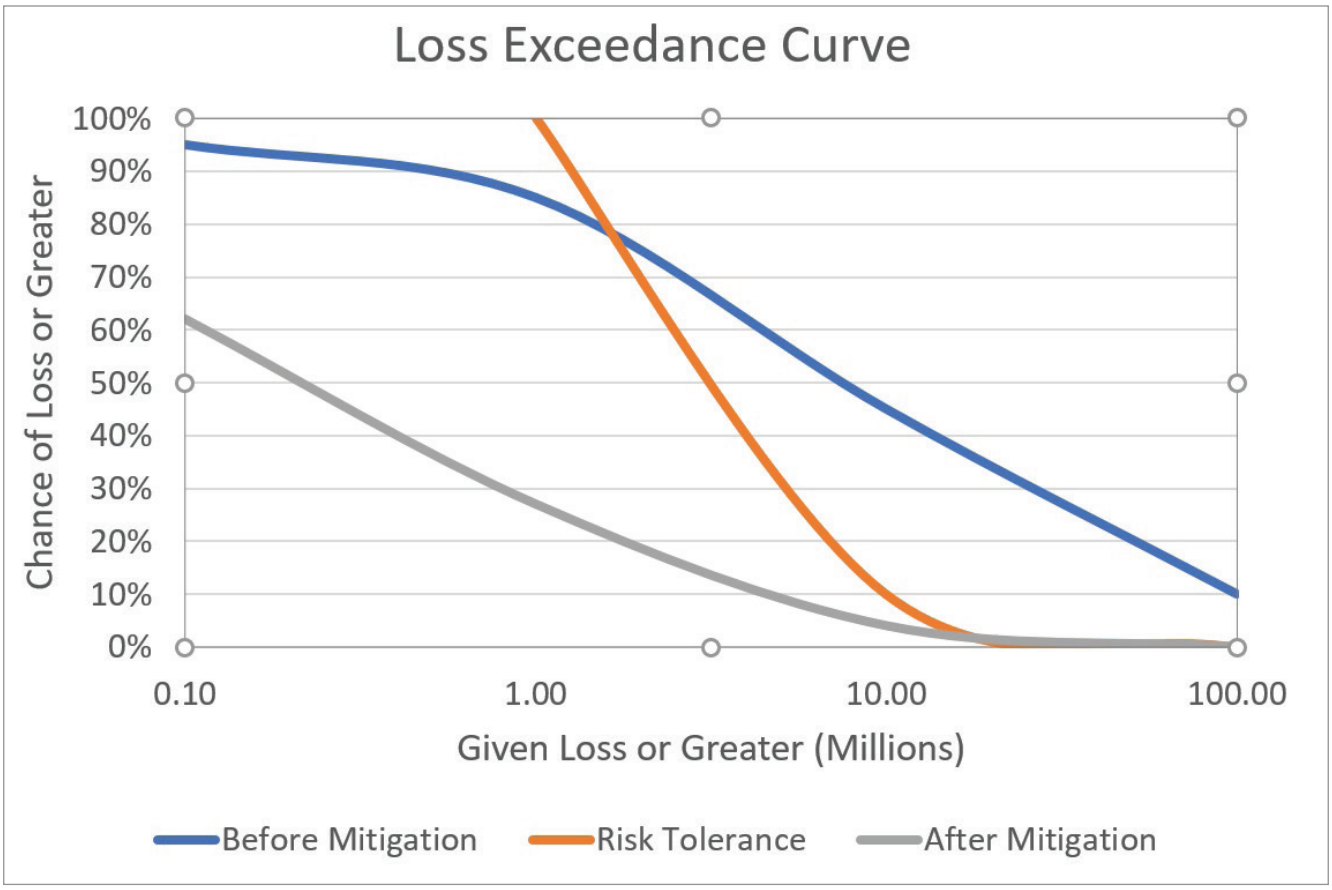
Risk Type	Event Risk	CI Only	AV Only	Both	CI Low	CI High
Credential Reuse	100%	60%	30%	10%	$1,000	$25,000

Risk Type	Event Risk	CI Only	AV Only	Both	CI Low	CI High	Time Low	Time High	AV Low CPH*	AV High CPH*
Credential Reuse	100%	60%	30%	10%	$1,000	$25,000	50.0	300.0	$100	$250

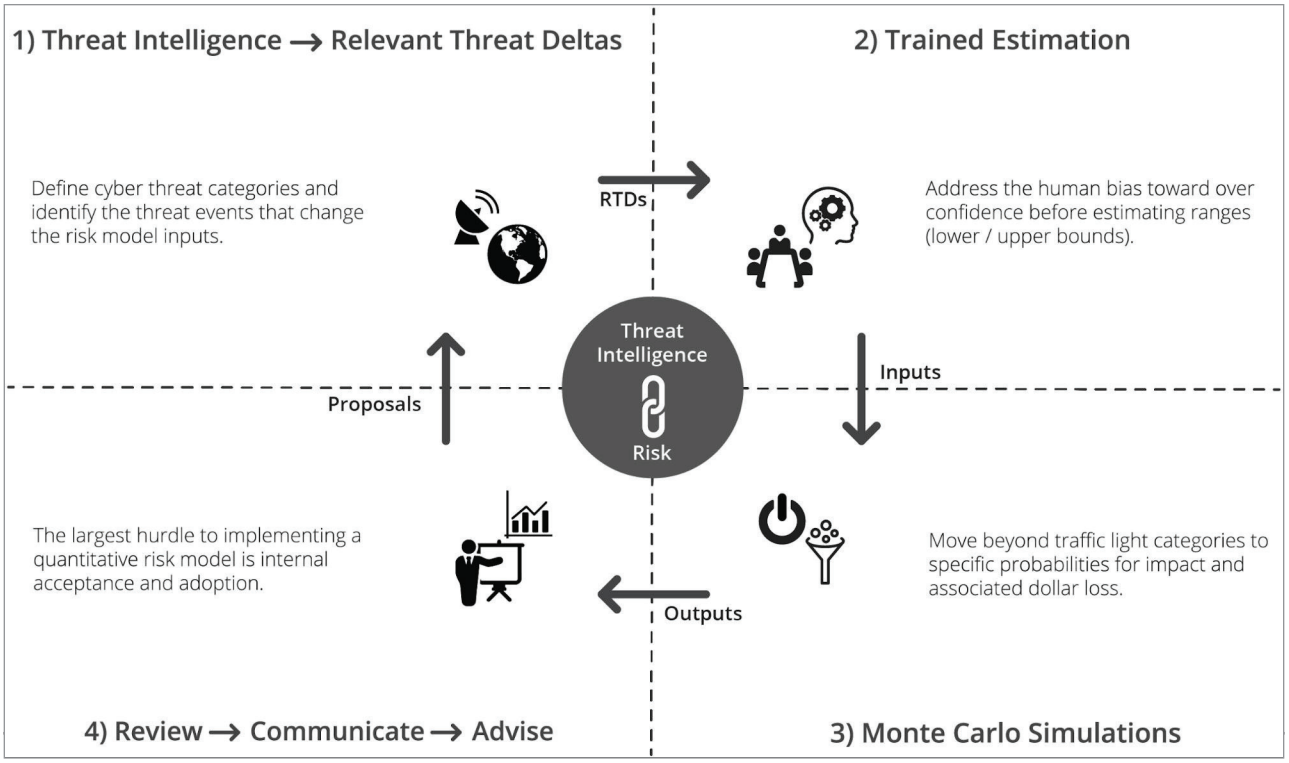
*Cost per Hour

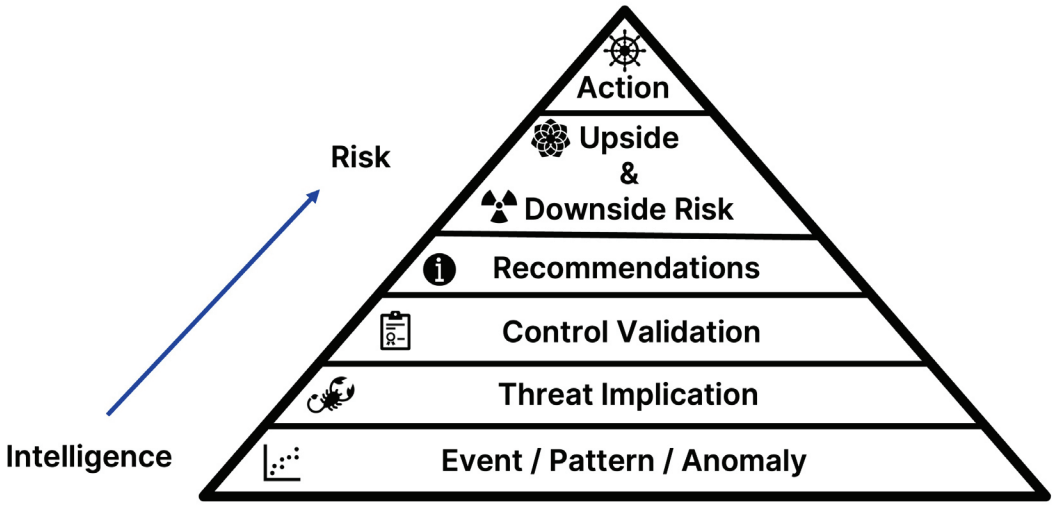
Risk Type	Event Risk	CI Only	AV Only	Both	CI Low	CI High	Time Low	Time High	AV Low CPH	AV High CPH
Social Engineering	100%	80%	10%	10%	$ 20,000	$ 250,000	1,200.00	3,000.00	$ 100	$ 250
Credential Reuse/Stuffing/Brute Forcing	100%	60%	30%	10%	$ 1,000	$ 25,000	50.00	300.00	$ 100	$ 250
Web Application Vulnerabilities	50%	40%	30%	30%	$ 5,000	$ 500,000	24.00	120.00	$ 500	$ 100,000
Denial of Service	5%	0%	100%	0%	-	-	1.00	24.00	$ 70,000	$ 240,000
Internet Protocol Hijacking (DNS/BGP)	5%	10%	80%	10%	$ 100	$ 1,000,000	.50	72.00	$ 10,000	$ 250,000
Hardware Vulnerabilities	50%	10%	60%	30%	$ 1,000	$ 1,000,000	3.00	336.00	$ 500	$ 100,000
Software Vulnerabilities (not web related)	100%	0%	100%	0%	-	-	50.00	1,500.00	$ 100	$ 500
Physical Tampering	10%	0%	90%	10%	$ 100	$ 1,000,000	.25	168.00	$ 500	$ 50,000

Probability of This Loss or Greater	Total CI Loss	Total AV Loss	Total Loss	Credential Reuse: Total Loss	Web Application Exploitation: Total Loss	Exploited Vulnerability: Total Loss	Phishing: Total Loss	Ransomware (Internal Workstations Only): Total Loss
95%	$48,932.98	$1,108,327.00	$1,251,663.00	$580,034.60	$0.00	$0.00	$217,901.40	$9,404.66
90%	$63,457.61	$1,242,980.00	$1,403,847.00	$657,155.40	$0.00	$0.00	$247,986.70	$14,276.62
85%	$75,957.43	$1,350,330.00	$1,522,604.00	$714,480.80	$0.00	$0.00	$270,497.70	$18,792.91
80%	$87,625.05	$1,444,638.00	$1,630,886.00	$763,884.80	$0.00	$0.00	$289,878.00	$23,510.41
75%	$99,539.46	$1,534,862.00	$1,734,583.00	$809,776.70	$0.00	$0.00	$307,783.70	$28,501.25
70%	$111,585.25	$1,625,478.00	$1,838,824.00	$852,792.00	$0.00	$0.00	$324,799.00	$33,866.94
65%	$124,293.34	$1,719,219.00	$1,945,519.00	$894,525.00	$0.00	$0.00	$341,176.70	$39,657.47
60%	$137,632.16	$1,817,014.00	$2,059,930.00	$935,650.50	$0.00	$0.00	$357,726.00	$45,961.65
55%	$152,428.25	$1,924,844.00	$2,182,548.00	$977,639.10	$0.00	$0.00	$374,549.50	$53,213.17
50%	$168,940.79	$2,044,278.00	$2,320,317.00	$1,020,942.60	$14,674.47	$0.00	$391,791.10	$61,335.51
45%	$187,401.55	$2,181,988.00	$2,477,782.00	$1,064,832.10	$101,975.60	$45,128.89	$409,867.10	$70,839.06
40%	$209,070.60	$2,341,963.00	$2,666,050.00	$1,113,015.90	$174,960.29	$93,787.96	$429,149.10	$82,037.47
35%	$234,614.25	$2,538,985.00	$2,892,137.00	$1,165,631.10	$260,710.40	$160,561.43	$449,759.60	$95,359.09
30%	$266,081.91	$2,794,515.00	$3,178,194.00	$1,223,398.50	$373,392.09	$254,378.97	$473,006.80	$111,632.72
25%	$306,010.38	$3,136,882.00	$3,570,372.00	$1,288,149.30	$524,224.21	$395,223.73	$499,291.50	$132,252.68
20%	$361,115.69	$3,633,943.00	$4,110,297.00	$1,363,878.70	$747,733.01	$616,575.30	$530,187.90	$160,353.11
15%	$442,934.33	$4,425,370.00	$4,966,129.00	$1,459,628.40	$1,094,014.58	$1,010,318.04	$569,239.00	$200,229.88
10%	$586,292.40	$5,885,030.00	$6,496,379.00	$1,589,005.90	$1,754,853.29	$1,828,368.38	$622,563.20	$265,061.73
5%	$948,516.43	$9,657,421.00	$10,436,777.00	$1,801,617.20	$3,451,042.16	$4,297,746.59	$710,808.00	$401,099.91
1%	$2,984,718.46	$29,677,965.00	$31,066,102.00	$2,289,354.70	$11,883,288.27	$20,592,835.66	$918,448.80	$871,851.70



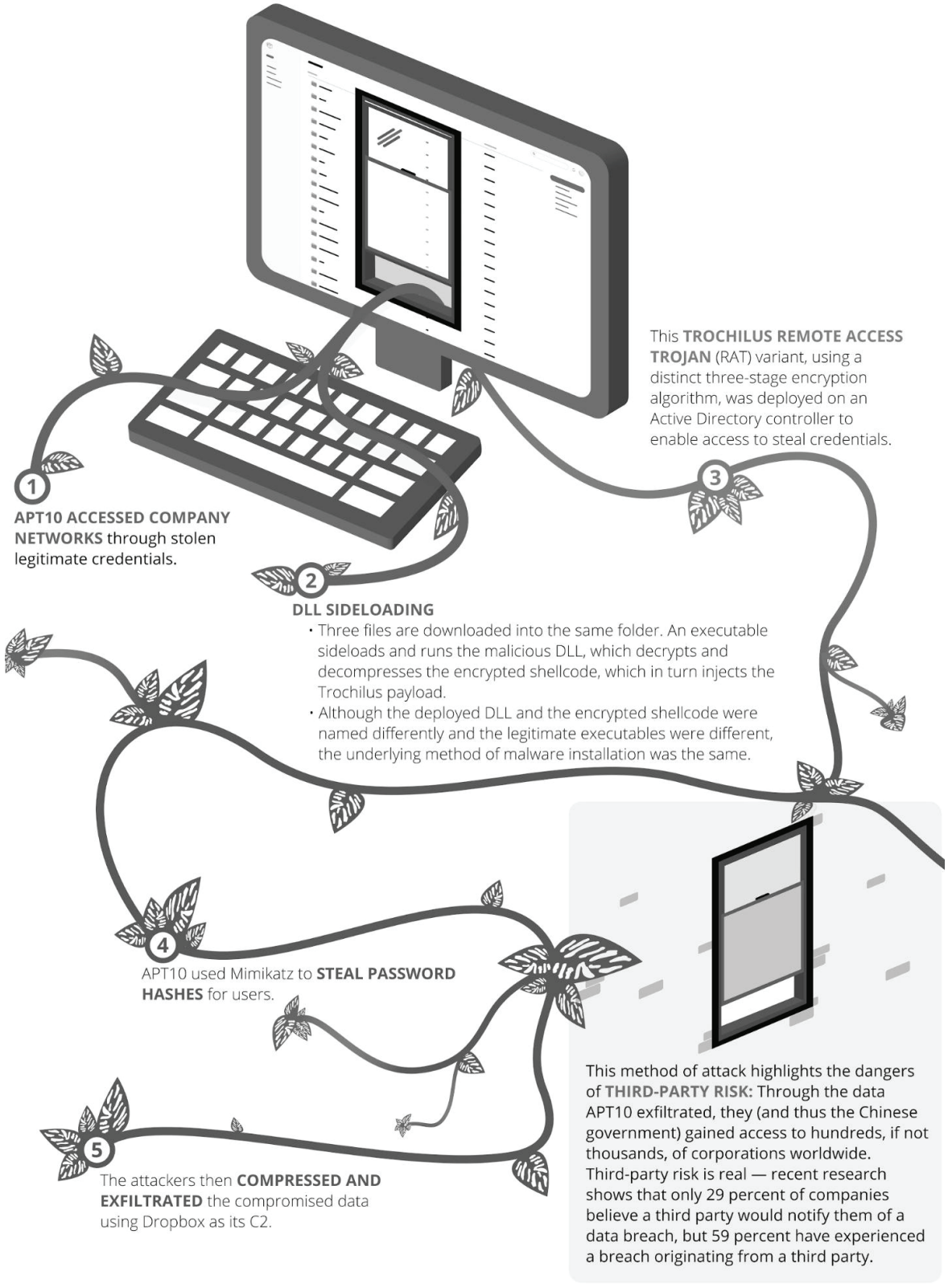
Example of a loss exceedance curve (Source: Paul Stokes articles on the World Economic Forum website: https://www.weforum.org/agenda/2019/07/can-cybersecurity-offer-value-for-money/.)


1) Threat Intelligence → Relevant Threat Deltas
2) Trained Estimation
Define cyber threat categories and identify the threat events that change the risk model inputs.
RTDs
Address the human bias toward over confidence before estimating ranges (lower / upper bounds).
Threat Intelligence
Risk
Proposals
Inputs
The largest hurdle to implementing a quantitative risk model is internal acceptance and adoption.
Outputs
Move beyond traffic light categories to specific probabilities for impact and associated dollar loss.
4) Review → Communicate → Advise
3) Monte Carlo Simulations

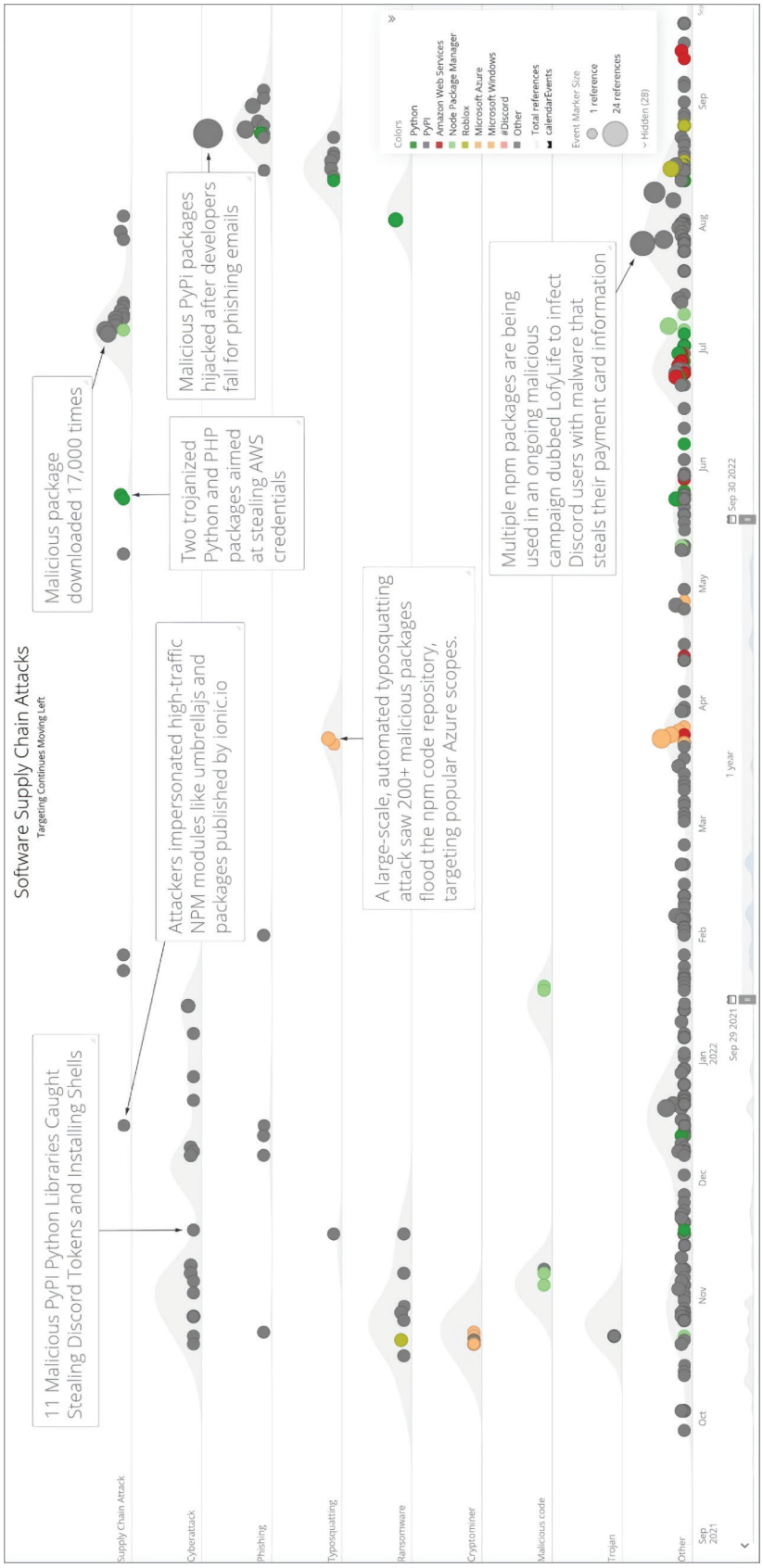

Risk
Intelligence
Action
Upside & Downside Risk
Recommendations
Control Validation
Threat Implication
Event / Pattern / Anomaly

Problems	Potential Breach Notification	Infrastructure Exposure Identification	Physical Harm Avoidance	Quick Attack Remediation	Vulnerability Exploitation Avoidance	Fraud Avoidance	Credential Unauthorized Access	Supply Chain Liability	Security Control Efficacy
Intelligence	• Phishing domains • Malicious apps • Code leaks • DW access advertising	• Internet inventory • Asset exposures	• Terrorist campaigns • Executive/ asset threats • Travel risk	• IOA/IOC context and enrichment • Infrastructure compromises	• Active exploitation • Pre-NVD • Pre-CVSS	• Stolen payment cards • Merchant breaches • Proxy/VPN use	• Stolen credentials/ tokens	• Vendor/ supplier exposure analytics	• Adversary prioritization • Hunting packages • New "tools"/ TTPs
Consumption	• Email reporting • API	• API system integration • Email alerting	• Alerting • Geospatial monitoring • API system integration	• Browser extension • System of record integration	• Scanner integration • System of record integration	• API system integrations • Manual reporting	• API for SOAR playbook	• System of record integration • Intelligence cards	• Red team scenarios • Hunting team scenarios
Outcomes	• Domain/social media/app store takedowns • Legal action	• Exposed asset remediation	• Site security • Business continuity response • Executive protection	• Quicker event verdicts • Faster incident triage • Detect/block control actions	• Patch prioritization	• Active cards flagged • Account takeover prevention	• Active Directory/ Cloud account resets	• Vendor/ supplier contract auditing/ enforcement	• Security control validation • Internal threat discovery • Trend identification
KPIs	• Mean time to remove • ROSI	• New assets discovered • ROSI	• Physical/ operational system disruption • ROSI	• Correlated detection events • ROSI	• Patch escalation • ROSI	• Cost of fraud • Approved vs. declined transactions • ROSI	• Mean time to identify • ROSI	• Exposure identification • ROSI	• Mean time to assess • Mean time to deploy • ROSI
Risk Briefing	• NIST CSF: DE.CM-5 DE.CM-7 • Reputation management	• NIST CSF: ID.AM1-4 • Reduce breach probability • Risk reduction	• NIST CSF: DE.CM2-3 • Improve resilience	• NIST CSF: DE.AE2-3 DE.CM-1 • Improve resilience • Regulatory compliance	• NIST CSF: ID.RA-1 PR.IP-12 • PCI DSS • Regulatory compliance	• PCI DSS • Regulatory Compliance • Improve brand equity	• NIST CSF: PR.AC1-7 • Risk reduction • Regulatory compliance	• NIST CSF: ID.SC1-5 DE.CM-6 • Risk reduction • Regulatory compliance	• NIST CSF: ID.RA2-5 DE.CM-4 • Improve risk assessments

Recorded Future



The TTPs APT10 used to breach Visma's systems.
Source: https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf



A timeline of supply chain attacks, September 2021 to September 2022 (Source: Recorded Future)

About the Author

Levi Gundert is Recorded Future's chief security officer, a role in which he leads the continuous effort to measurably decrease operational risk both internally and for clients. Levi has spent the past 20 years in both the public and private sectors, defending networks, arresting international criminals, and uncovering nation-state adversaries. Levi previously led senior information security functions across technology and financial enterprises. He is an author, a trusted risk advisor to Fortune 500 companies, and a prolific speaker, blogger, and columnist.