19th New York State Cyber Security Conference Presentation, Albany, NY
June 8 - 9, 2016, Empire State Plaza - Albany, NY

CyberFinance: Why Cybersecurity Risk Analytics must Evolve to Survive 90% of Emerging Cyber Financial Threats, and, What You Can Do About It?

Advancing Beyond 'Predictive' to 'Anticipatory' Risk Analytics

Yogi

Dr. Yogesh Malhotra
PhD, MSQF, MS-CS, MS-NCS, MS-Acc, MBA-Eco, C.Eng., CISSP, CISA, CEH, CCP/CDP
Who's Who in America®, Who's Who in the World®,
Who's Who in Finance & Industry®,
Who's Who in Science & Engineering®
www.yogeshmalhotra.com
dr.yogesh.malhotra@gmail.com

www.its.ny.gov

FinRM™
Global Risk Management Network, LLC,
757 Warren Rd, Cornell Business & Technology Park, Ithaca, NY 14852-4892
Phone: 646-770-7993

"The **new business model** of the Information Age, however, is marked by **fundamental, not incremental, change**. Businesses **can't plan long-term**; instead, they **must shift** to a more flexible **"anticipation-of-surprise" model**."
-- Dr. Yogesh Malhotra in ***CIO Magazine*** interview, Sep. 15, 1999.

CIO

Presenter's biography

Dr. Yogesh Malhotra: Top-10 PhD IT & Statistics Double Doctorate Computer Scientist with 35 SSRN Top-10 Research Rankings for 2015-2016 World Leading Cybersecurity and Finance Computational Quantitative Risk Analytics Research. 2016 & 2015 Princeton Quantitative Trading Conference Invited Presentations on Cybersecurity, CyberFinance, and, Computational Statistics Algorithms. Recently pioneered Quantitative Finance and Cybersecurity Risk Insurance Modeling research and practices that pre-empted and prevented the Global Insurance Crisis owing to mismeasurement and misestimation of Cyber Risk Insurance Modeling Losses given reliance of worldwide firms upon inappropriate Quantitative Risk Models based upon VaR. The specific venture advanced Quantitative Finance research in Model Risk Management with oversight of distinguished Cybersecurity experts and Computer Scientists affiliated with the U.S. Air Force Research Lab, New York State Cyber Research Institute, and, SUNY. That venture advanced upon top management project leaderships in Quantitative Finance Risk Modeling practices guiding top leadership Global Head of Risk & Analytics and US Head of Portfolio Management and associated Managing Directors for top Wall Street investment banks with $1 Trillion AUM such as JP Morgan Private Bank. Before that advanced worldwide global practices in Enterprise Risk Management and Model Risk Management by developing Anticipatory Risk Analytics frameworks of Model Risk Management a decade ahead of articulated need by Wall Street CFOs and CROs for such frameworks in the aftermath of the Global Financial Crisis. Prior to that founded award-winning influential financial, risk, and analytics ventures with CxO clients and patrons such as Goldman Sachs, Google, Harvard, IBM, Intel, Microsoft, MIT, and, UPMC. Founded ventures applied and recommended by world's leading visionary IT-CxOs such as Microsoft founder Bill Gates, Big-4 CxOs, and, top Commanders and CxOs of US Army / US Navy / US Air Force / US Air Force Research Lab. Research Impact ranked among Finance & IT Nobel Laureates in AACSB & Global Scientific & Industry Studies.

Summary of the session

This presentation advances upon recent world leading Cybersecurity-CyberFinance Computational Risk Analytics Research selected for 35 SSRN Top-10 Research Rankings and invited for presentations at the 2015 and 2016 Princeton Quantitative Trading Conference sponsored by the Princeton University, Goldman Sachs, and, Citadel. The primary focus of the presentation is on helping advance insights of auditors, business managers, critical infrastructure owners, educators, executives, information security professionals, forensic specialists, IT professionals, law enforcement, process improvement managers, and project managers about advancing beyond Retrospective and Predictive Risk Analytics to Anticipatory Risk Analytics. Using the metaphor of the iceberg with 90% of emerging cyber financial threats *invisible to human eye*, it sheds light on emerging Cyber risks that threaten the Financial survival of national and regional economies, global and local business enterprises, information infrastructure entities as well as individuals.

Backed by research ranked for worldwide impact among Finance and IT Nobel laureates, this presentation will help you see Cyber risk and its implication for Finance at various levels like you have never seen before. It advances upon industry-leading research that recently developed robust foundation of global Cyber Risk Insurance standards with oversight of Cybersecurity experts affiliated with U.S. Air Force Research Lab and New York State Cyber Research Institute.

The presentation builds upon global leadership of professional hi-tech practices in global Banking and Finance industry over the recent 25 years with most recent risk analytics leadership for top Wall Street investment banks such as JP Morgan, FinTech risk analytics ventures with CxO clients and patrons such as Goldman Sachs, and, prior global leaderships for Big Banks such as Bank of America and Big-3 IT firms leading global financial systems development for worldwide Banking & Finance firms.

20-Years Leading Global Research & Practices in Advancing Beyond 'Predictive' to 'Anticipatory' Risk Analytics

http://FinRM.org/

"The **new business model** of the Information Age, however, is marked by **fundamental, not incremental, change**. Businesses **can't plan long-term**; instead, they **must shift** to a more flexible **"anticipation-of-surprise" model**."
-- Dr. Yogesh Malhotra in ***CIO Magazine*** interview, Sep. 15, 1999.

CIO

Anticipatory Risk Analytics: Growing Awareness

SANS

"Organizations need anticipatory, active defenses designed to frustrate, annoy and deceive advanced **adversaries** (and **insiders**) who have already achieved access to their innermost sanctums." – SANS Institute October 6, 2015, *InfoSecurity Magazine*
To Stop APTs You Need Anticipatory Active Defenses

RSA

"Data drives decision making for people and computer systems. When that data is unknowingly [**or knowingly**] manipulated, those decisions will be made based on false data.... The advent of connected and automated sensors aggressively exacerbates these issues."
– RSA, Dec. 10, 2015, SiliconAngle NewsLetter

CGI

"The other aspect is digital transformation and the computerization of everything. .. One of the key things in cybersecurity is not just about there being more bad guys out there, but that the different kinds of cyber and information technology entry points are growing [**exponentially**] all the time." – Homeland Preparedness News, May 27, 2016

References: Recent Research

- Risk, Uncertainty, and Profit for the Cyber Era: 'Knight Reconsidered'

- Beyond Model Risk Management to Model Risk Arbitrage for Fintech Era
- Future of Finance Beyond 'Flash Boys': Risk Modeling for Managing Uncertainty
- Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management
- Markov Chain Monte Carlo Models, Gibbs Sampling, & Metropolis Algorithm
- Cybersecurity & Cyber-Finance Risk Management: Threats & Vulnerabilities
- Measuring & Managing Financial Risks with Improved Alternatives beyond VaR
- A Risk Management Framework for Penetration Testing of VoIP Protocols
- Quantitative Modeling of Mobile Trust and Trust Management Protocols
- Number Field Sieve Cryptanalysis Algorithms for Prime Factorization

http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=2338267

Data: The 'Currency' of the Cyber Era

In the Networked Era of Bits and Bytes... Going soon to 'Qubits'...

DATA **is** 'Value', 'Valuation', 'Money', 'Price', 'Payment', 'Transaction'

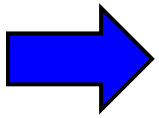
DATA **is** direct access to CONTROL rather than **via** 'Money'

DATA **is** direct access to OWNERSHIP rather than **via** 'Money'

Finance: Economies, Markets, Exchanges, Payments, Transactions

Infra: Telecom, Finance, Healthcare, Energy, Industry, Transportation

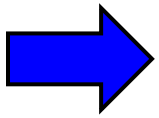
Data Access
Data Integrity
Data Validity
Data Reliability



Networks

Applications

Hosts



Data Driven Decision Making

http://cloudcomputing.sys-con.com/

Anticipating Human-ICT Vulnerability Exploits

"Microsoft's Threat Research & Response blog issued an alert to its customers on May 26 warning them of the bug, which also goes by the name ZCryptor. The nastiest aspect of this piece of malware is its ability to reproduce and then spread to other systems through removable media devices, such as flash drives, as well as network drives..."

Anticipate This!!

Stuxnet

IEEE SPECTRUM

http://www.wired.com/2015/01/blackhat-the-best-cyber-movie/

Beyond 'Predictive' to 'Anticipatory' Risk Analytics

'What gets measured, gets managed.' – Peter Drucker

Yogesh Malhotra's Analytics Corollaries:

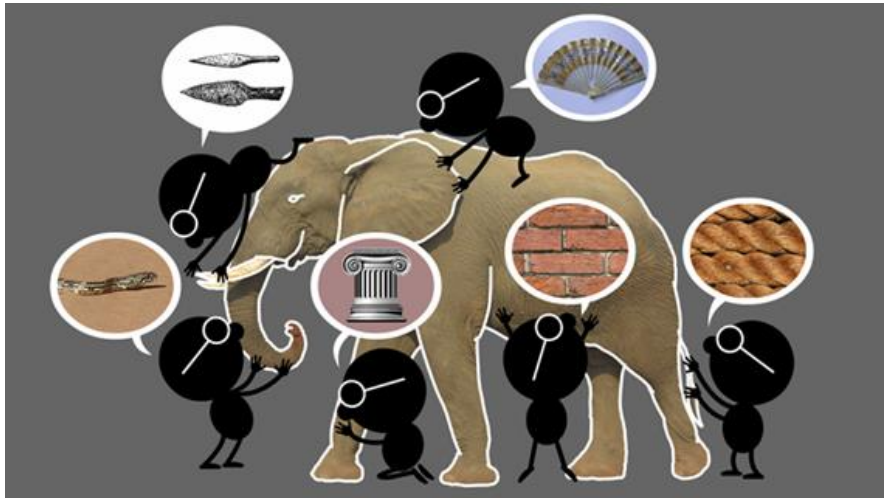
'On the folly of rewarding A, while hoping for B' – Steve Kerr

What gets mismeasured, gets mismanaged.

What gets mostly mismeasured, gets mostly mismanaged.

Two Guiding Questions on *Prediction*: IT, Statistics, Controls.

"Driving forward by looking through the rear-view mirror..."
- ISR's description of the IS field, 1993



"**Models are backward-looking**." – Wall Street CEOs after the 'Crisis' of 2008-2009

"The **new business model** of the Information Age, however, is marked by **fundamental, not incremental, change**. Businesses **can't plan long-term**; instead, they **must shift** to a more flexible **"anticipation-of-surprise" model**."
-- Dr. Yogesh Malhotra in ***CIO Magazine*** interview, Sep. 15, 1999.

CIO

Advancing Beyond 'Predictive' to 'Anticipatory' Risk Analytics

CyberFinance: Why Cybersecurity Risk Analytics must Evolve to Survive 90% of Emerging Cyber Financial Threats, and, What You Can Do About It?

1. 20-Years of Anticipatory Risk Analytics
2. *Griffiss Cyberspace*™ and Cyber 9-11
3. RSA1024 'Gold Standard' Shattered
4. Mis-measure of Cyber Risk @ CERT
5. Cyber Risk Industry Mis-measure of Risk
6. Cyber déjà vu of Global Financial Crisis
7. Global Cyber Insurance Crisis Averted
8. Materiality of Cyber Risk, Lack Thereof
9. The Cyber-Finance-Trust Framework
10. Beyond Mis-measure of Cyber Risk
11. The 'Iceberg' of Cyber-Finance Risk
12. '*Uncharted Territories*' of Cyber-Finance
13. Beyond Risk to Managing Uncertainty
14. Beyond NHST-Determinism to Bayesian
13. Bayesian & Markov Chain Monte Carlo
14. Increasingly Vulnerable Time and Space
15. Vulnerable Digital & Crypto-Currencies
16. 20-Years of Digital Transformation Models
17. Exponentially Growing Vulnerabilities
18. Black Hat Finance of FinTech Models
19. Assume Breach & Crypto-Apocalypse
20. Healthcare More Vulnerable than Finance?
21. Healthcare: Following Finance Analytics?
22. Vulnerable Digital and Virtual Economy
23. Toward Managing Catastrophic Risks
24. Modeling Catastrophic Risks
25. Additional Models and References

Advancing Beyond 'Predictive' to 'Anticipatory' Risk Analytics

Download Related Research from: http://www.yogeshmalhotra.com/blackswans.html

From 'Prediction' to "Anticipation of Surprise"

"The future is moving so quickly that you can't anticipate it… We have put a tremendous emphasis on quick response instead of planning…
We will continue to be surprised, but we won't be surprised that we are surprised. ***We will anticipate the surprise."***

Goldman Sachs

Goldman Sachs CEO Lloyd Blankfein told the Australian Institute of Company Directors at a breakfast briefing on Friday, July 26 2013, how investors should prepare for the most extreme risk scenario. His comments about risk management capture the essence of the 'anticipation of surprise' model mentioned above and explained in Dr. Yogesh Malhotra's research papers and research monographs published over the last decade or so.

"The future is moving so quickly that you can't anticipate it… We have put a tremendous emphasis on quick response instead of planning. We will continue to be surprised, but we won't be surprised that we are surprised. We will anticipate the surprise." - Anticipation of Surprise Framework

Risk Management Analytics beyond 'Prediction' to 'Anticipation of Risk'™ (1993-Current)
On the Origin of the Model Risk Management (MRM) Research Program

Goldman Sachs

Goldman Sachs

1993-Current

"The **new business model** of the Information Age, however, is marked by **fundamental, not incremental, change**. Businesses **can't plan long-term**; instead, they **must shift** to a more flexible **"anticipation-of-surprise" model**."
-- Dr. Yogesh Malhotra in ***CIO Magazine*** interview, Sep. 15, 1999.

CIO

that concept into a comprehensive and actionable framework of ***model risk management*** *of non-deterministic risks such as those associated with black swans through '****anticipation of surprise****' by '****effective challenge of models****'....*

...Over subsequent years, Yogesh Malhotra's influential research and practices on realizing and executing the cyberspace era vision of risk modeling and risk management have guided world's digital social enterprise has been already developing frameworks and models for the anticipated ***future of finance*** *and* ***future of risk*** *starting with the first WWW-browser in 1993... adopted by worldwide firms, governments, and institutions... and written about and recommended by greatest tech visionaries such as Microsoft founder Bill Gates...*

...Whether you are a pioneer in the ***ERM*** *and* ***MRM*** *game or just getting started, you are all "welcome to the new world of*

Griffiss Cyberspace™ and Cyber 9-11

Griffiss Cyberspace (GriffissCyberspace.com) Cybersecurity Venture Aims to Span Wall Street and Hi-Tech Research: World-Leading Thought Leadership of Global Defense Bearing on Global Finance Cybersecurity

Griffiss Cyberspace, our latest Cyber Risk Management venture in the Griffiss Air Force Base area of Rome, New York, advances our global CxO leadership renowned for pioneering U.S. and worldwide risk practices in IT and Cyber Risk Management. It aims to connect the dots between Wall Street quantitative finance and quantitative risk modeling research and practices and latest generation computational and mathematical research and practices in cybersecurity and cyber risk management of critical national information infrastructures (NII). Its socioeconomic objective is to contribute to the regional economic development of Central New York and advancement of cybersecurity and cyber risk management practices related to global banking and financial systems and other critical NII.

Our prior research followed by the nation's top signals intelligence (SIGINT) expert agencies NSA and CIA, such as the computer science journal *Expert Systems with Applications* top-ranked paper on Cyber risk management human and machine learning expert systems & AI (2001), advanced upon Shannon's Information Theory. Inspired by our communication with the Genetic Algorithms pioneer Dr. John Holland (1995) at the Santa Fe Institute at the time, it anticipated and addressed many questions raised about quantitative computational models in the aftermath of the 2008-2009 Global Financial Crisis more than a decade ahead of time. Our recent Cryptanalysis research focus on Number Field Sieve Cryptanalysis Algorithms for Prime Factorization on Composites proposed next generation robust encryption standards by

Malhotra, Y., Expert Systems for Knowledge Management: Crossing the Chasm between Information Processing and Sense Making, Expert Systems with Applications: An International Journal, 20(1), 7-16, 2001. http://www.brint.org/expertsystems.pdf

Reflecting on OCC's remark that the specific cyberattack and cybersecurity related risks represent 'operational risks', it seems important to update our perspectives characterizing financial risks in traditional terms such as Credit Risks, Market Risks, Operational Risks, etc. Such definitions might have reflected the *true nature* of financial risks in the past. Almost all risks characterizing *today's information-based financial products and services, financial markets, financial exchanges, financial currencies, and financial economies* are however first and foremost Information risks and Cyber risks. Such Information risks and Cyber risks may not only escalate traditional risks but may also subsume traditional financial risks as brick-and-mortar institutions such as NYSE 'trading floors' become 'museums of financial history'.

- Dr. Yogesh Malhotra, **Summer, 2013**

http://www.yogeshmalhotra.com/GriffissCyberspace.html

Griffiss Cyberspace™ and Cyber 9-11

"On Monday afternoon, seven New York State senators gathered at the Griffiss Institute for a cyber security hearing. The hearing, entitled Defending New York from cyber attacks covered various topics within the cyber security spectrum. There are six subcommittees under the cyber security topic: Banking, Veterans, Homeleand Security & Military Affair, Insurance, Commerce, Economic Development & Small Business, Crime VIctims, Crime & Correction, Select Committee on Science, Technology, Incubation & Entrepreneurship."

ROME OBSERVER
Taking a Good look at Rome & all of Oneida County www.RomeObserver.com

- **Cyber security conference held On Griffiss, *Rome Observer***, Monday, November 18, 2013.

Benjamin Lawsky, superintendent of the New York Department of Financial Services, said that cyberterrorism is the most significant issue that DFS will work on in the next year, saying the possibility of an "armageddon-like" cyberattack is one of his primary concerns as a financial regulator. "I worry that we're going to have some sort of major cyber-event in the financial system that's going to cause us all to shudder," Lawsky said... "We like to say that to some extent the failures to detect the 9/11 plot were a failure of imagination and communication," he said. "I'm worried about the same thing here—that an event will happen and we'll look back and say, 'How did we not do more?'

-- **NY regulator warns against looming cyber 9/11, CNBC, Sep 22 , 2014 12:47 p.m. ET**.

http://www.yogeshmalhotra.com/GriffissCyberspace.html

http://www.yogeshmalhotra.com/cyberrisk.html

RSA1024 'Gold Standard' Shattered

Dr. Malhotra underscores growing Cyber-Finance Risk for Global Banking, Finance & Insurance (BFSI): Excerpt from his presentation 15 miles from Air Force Research Laboratory (AFRL)

"First, based on available evidence, it is not improbable that the **current officially "recommended" most widely used global standard of encryption [1024-bit RSA] may have already been compromised**. Second, **it would *not* really be a 'surprise'** given that the infamous '40 quadrillion years' challenge for an earlier version of the standard was unraveled in mere 17 years. Third, given recent multi-billion dollar global Finance deals blown by compromise of such technologies, **it is increasingly *critical* to recognize the *exponentially increasing* cybersecurity risk among other Financial Risks**." -- Dr. Yogesh Malhotra in **Number Field Sieve Cryptanalysis Algorithms for Most Efficient Prime Factorization on Composites** presentation, **May 1, 2013**. *Related Paper published online on May 3, 2013*:
Malhotra, Y. **Cryptology beyond Shannon's Information Theory: Preparing for When the 'Enemy Knows the System' with Technical Focus on Number Field Sieve Cryptanalysis Algorithms for Most Efficient Prime Factorization on Composites**, Griffiss Cyberspace, Global Risk Management Network, LLC, **May 3, 2013**.

http://ssrn.com/abstract=2553544

"**Google** just announced that its HTTPS web pages **will be ditching 1024-bit RSA keys** in favour of 2048 bits." - Anatomy of a change - **Google** announces it will double its SSL key sizes, ***nakedsecurity***, **May 27, 2013**.

Google

http://www.yogeshmalhotra.com/cyberrisk.html

Mis-measure of Cyber Risk @ CERT

CyberV@R: A Model to Compute Dollar Value at Risk of Loss to Cyber Attack

http://www.cert.org/flocon/2013/presentations/ulrich-james-cybervar.pdf

In finance, trading desks maintain Value at Risk (VaR) models for measuring portfolio loss exposure.

A VaR model answers the question "what is the amount of money $\$X$, such that the odds of losing more than $\$X$, over time window T, fall below some threshold of probability P?" We call this the "P-percent VaR."

The most vanilla case (c.f. [Hull2000]) involves a portfolio of two stocks A and B. If we know (in \$) the daily volatility σ_A and σ_B of the stock prices, and the correlation coefficient ρ describing how they move relative to each other, (typically derived from historical data), then the P-percent VaR[2] is the value of X such that:

$$\frac{P}{100} = \frac{1}{\sigma_{AB}\sqrt{2\pi}} \int_{x=-\infty}^{x=X} e^{-x^2/2\sigma_{AB}}\, dx.$$

"Our analysis reveals that cyber risk entails exponentially higher **tail risks** and **systemic risks** thus making **VaR unfit for reliance** as the primary risk model for cyber insurance modeling."

Risk, Uncertainty, and, Profit for the Cyber Era:
Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics
http://ssrn.com/abstract=2553547

Measuring & Managing Financial Risks with Improved Alternatives Beyond Value-at-Risk (VaR)
http://ssrn.com/abstract=2594859

VaR & Beyond VaR for Cyber Risk Insurance

VaR: Amount of loss *not* to be exceeded in a *given time frame* with a *certain probability*.

Maximum amount of money likely to be lost over a *specific time period*, at a *specific confidence level*.

Theoretical basis of VaR is the portfolio theory and MVO.

Mean Variance Framework for Measuring Cyber Risk Loss

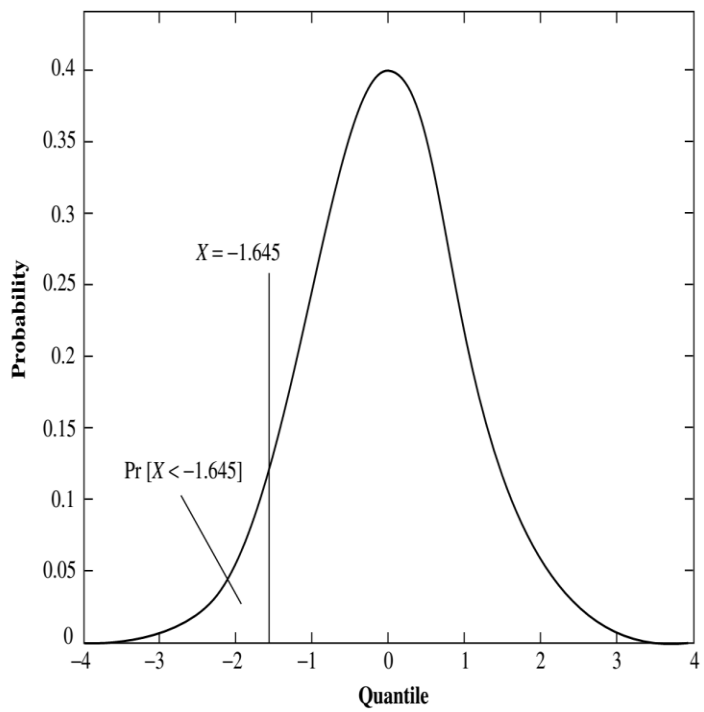
$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2}((x-\mu)/\sigma)^2\right]$$

http://ssrn.com/abstract=2553547

Mean Variance Framework for Measuring Cyber Risk of Expected Financial Loss

Normal pdf with $\mu = 0$ and $\sigma = 1$ known as a *standard normal*

$$f(x) = \frac{1}{\sqrt{2\pi}}\, e^{-\frac{1}{2}x^2}$$



standard normal variate

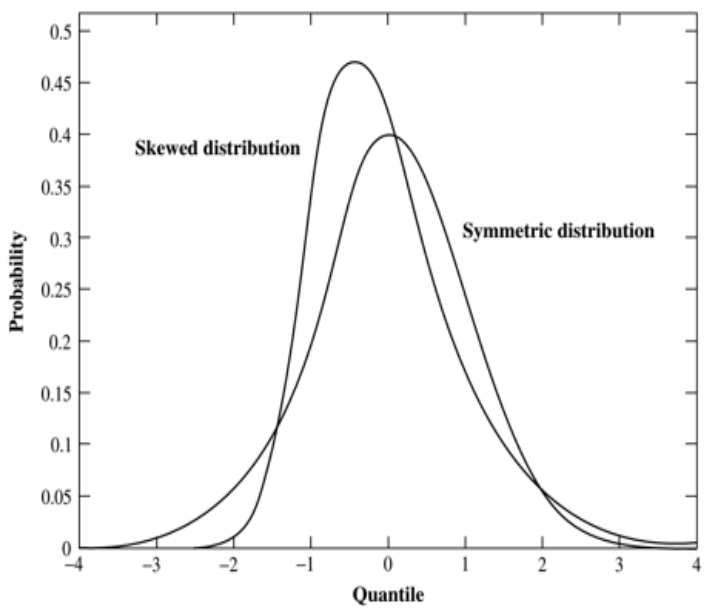
$$\alpha_{cl} = \frac{X_{cl} - \mu}{\sigma}$$

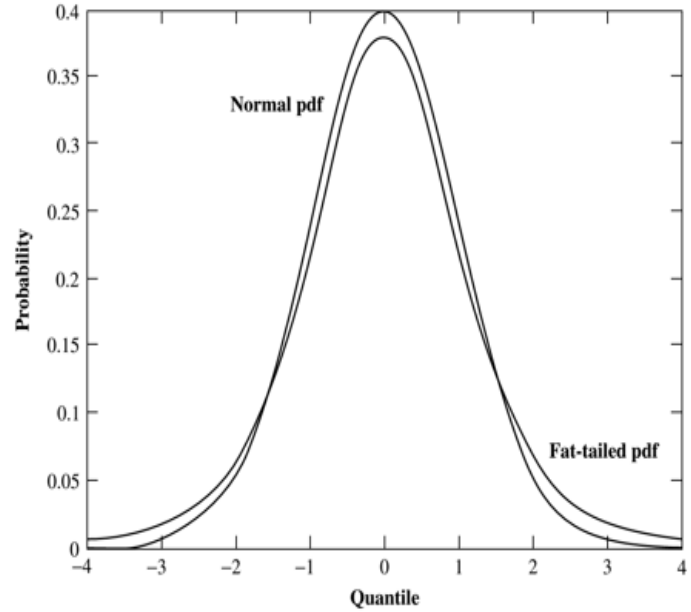
$$\Pr[x \le X] = \int_{-\infty}^{X} \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2}((x-\mu)/\sigma)^2\right] dx$$

http://ssrn.com/abstract=2553547

Skewness and Kurtosis Characterize 'Tail Risks' in Non-Normal Distributions

http://ssrn.com/abstract=2553547





$$Skew = E(x-\mu)^3/\sigma^3$$

$$Kurtosis = E(x-\mu)^4/\sigma^4$$

cyber risks are highly correlated and highly interdependent

For cyber risk, negative skew with a *left long tail* indicating *greater concentration of risk of loss.*

For cyber risk, *left fat tail* indicating *extreme events* more likely inflicting large losses particularly relevant

Value-at-Risk (VaR) for Cyber Risk Insurance Modeling

VaR is the maximum likely loss over some target period at a specified probability level.

Broadly speaking, VaR can be applied in various ways:

(a) as a point estimate measure of *maximum probabilistic loss*,

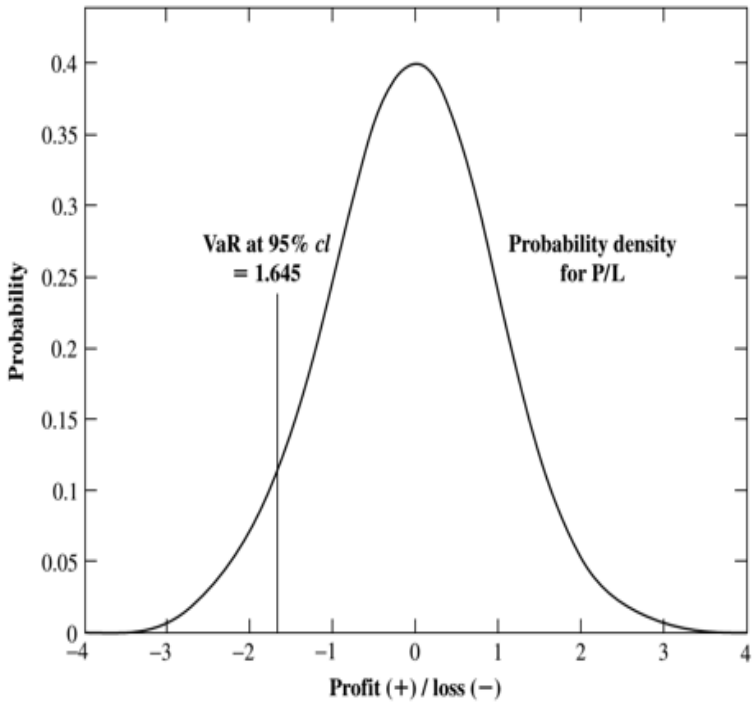
(b) as an *estimation procedure*,

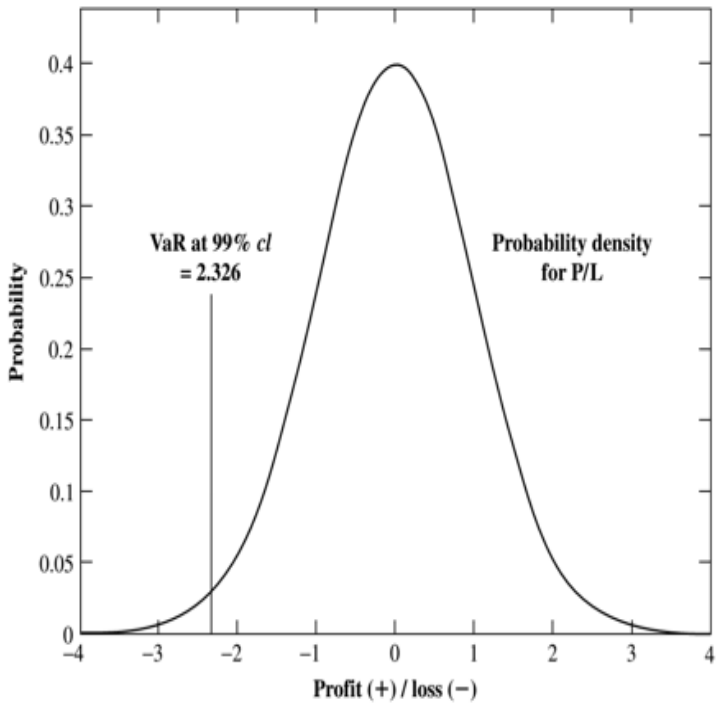
(c) as a *methodology* that can estimate other risks as well, and,

(d) as an *approach to risk management* for strategic decision-making.

http://ssrn.com/abstract=2553547

How Tail Risks Vary for Different Point Estimates of Normal VaR



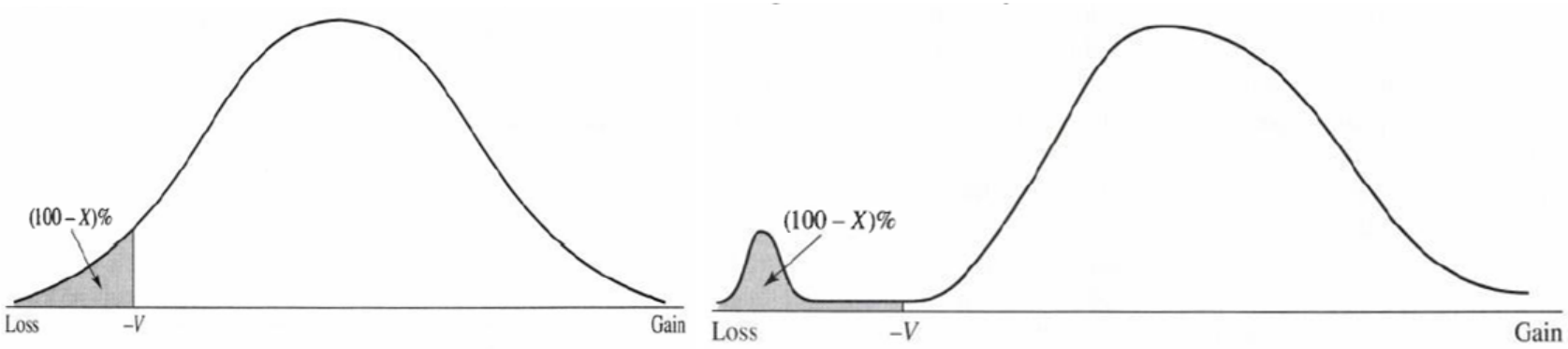


at the same confidence level, 5% of the time, the maximum cyber risk loss *can* exceed 1.645 σ

1% of the time, the maximum cyber risk loss *can* exceed 2.326 σ

http://ssrn.com/abstract=2553547

Why VaR is unable to Account for *Tail Risk*? *Because it is not so designed*



Left panel and the right panel both have the exact same VaR. However, the right panel shows ***non-normality*** in which the probability of risk is concentrated in the left tail, a ***fat tail*** resulting from a multimodal distribution.

VaR also treats risk as *exogenous*. Our analysis, however, established that cyber risks are not only highly *interdependent* and *correlated*, but can be also *endogenous* in nature.

http://ssrn.com/abstract=2553547

Cyber Risk Industry's Mis-measure of Risk

- "...Most prominent model being applied by most key players across diverse business economic and technology sectors is 'Value-at-Risk' model called VaR for short..."
- *VaR doesn't account for extreme risks in tails that can lead to 'catastrophic economic losses.'*
- VaR is *not* a systemic risk measure.
- *Lack of independence across diverse cyber risks and correlations as well as entities subject to cyber risks can result in significant systemic risk that VaR doesn't account for.*

Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics http://ssrn.com/abstract=2553547

Cyber déjà vu of Global Financial Crisis

RECIPE FOR DISASTER: THE FORMULA THAT KILLED WALL STREET

http://ssrn.com/abstract=2553547

- "If left unchecked and uncontrolled, large-scale commercial reliance upon VaR with its inherent model risks, tail risks, and systemic risks is expected to lead to impending national cyber risk and cyber-insurance disaster."
- "How can impending national cyber insurance modeling crisis be pre-empted and prevented?"
- "What can be possibly done to alleviate and minimize the model risk of unknowing and unquestioning appropriation of VaR model from finance into cyber insurance modeling?"

FINANCIER WORLDWIDE corporatefinanceintelligence

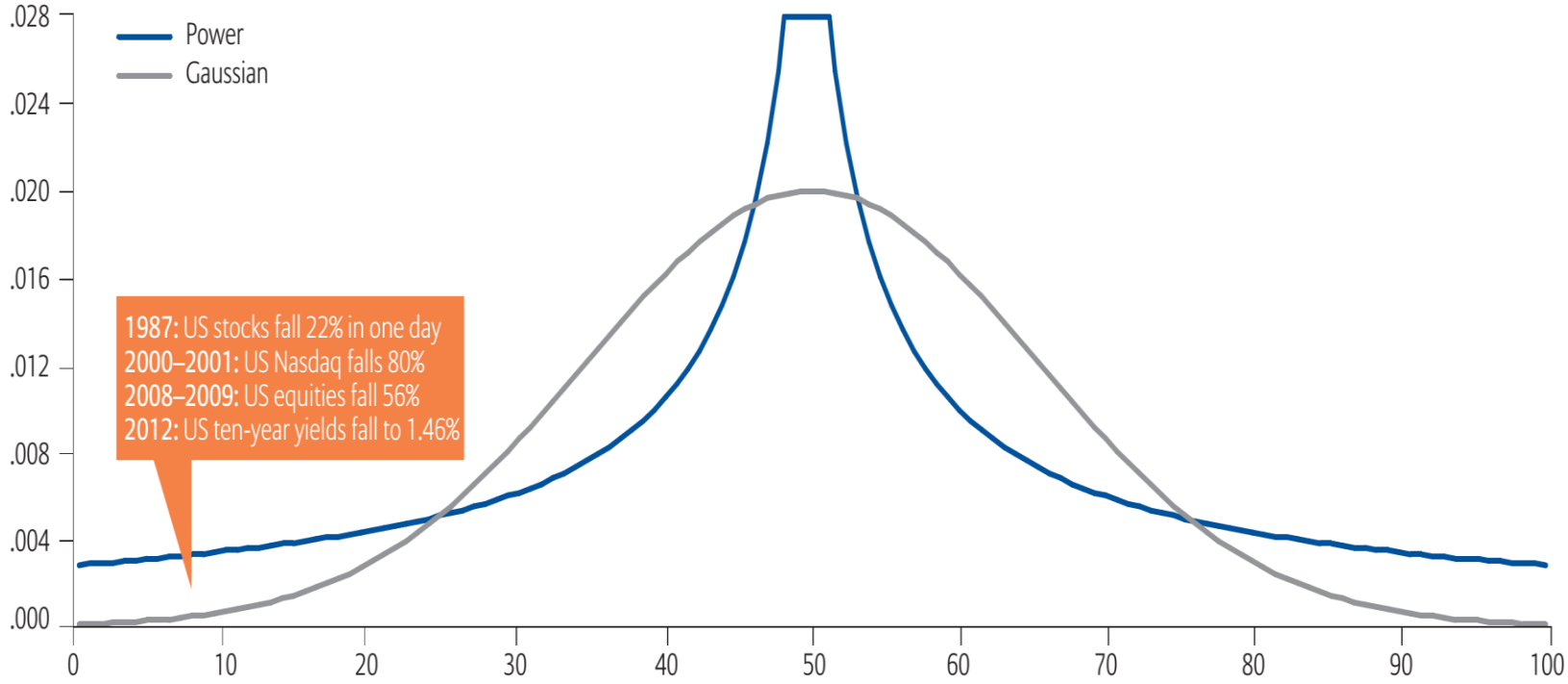
Clear and present danger: the pressing need to address cyber risk requires its better understanding and adequate quantification

August 2014 | SPECIAL REPORT: TECHNOLOGY IN BUSINESS

Financier Worldwide Magazine

Measuring & Managing Financial Risks with Improved Alternatives Beyond Value-at-Risk (VaR)
http://ssrn.com/abstract=2594859

Most of *Sociotechnical* World is *Non-Normal* and Governed by *Power Laws*



allianzgi.com

http://ssrn.com/abstract=2553547

Improved Alternatives beyond VaR and Toward Coherent Risk Measures

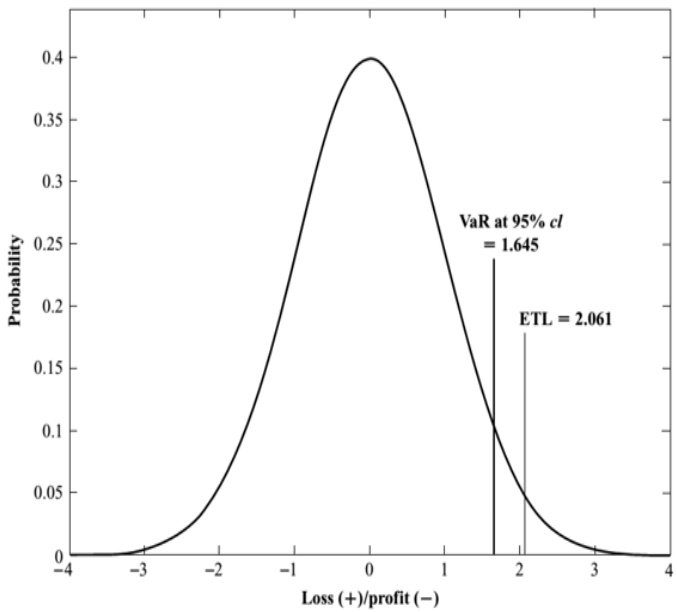
Sub-additivity of risk measure $\rho(.)$ implies that estimated loss from *combination* of risk A (e.g. spear phishing) and risk B (e.g. malware dropping) is less than or equal to the sum of potential losses from each of A and B considered separately on their own:

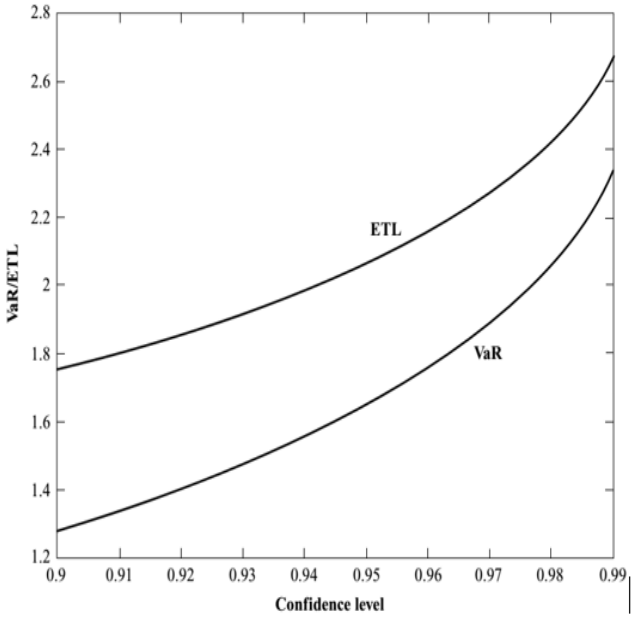
$$\rho(A + B) \leq \rho(A) + \rho(B)$$

May 2014 Report on Cyber Security in the Banking Sector by the New York State Department of Financial Services: "The larger the institution, the more likely it appeared to experience **malware** *and* **phishing** attempts."

http://ssrn.com/abstract=2693886

Expected Tail Loss (aka T-VaR and Expected Shortfall) as a Coherent Risk Measure



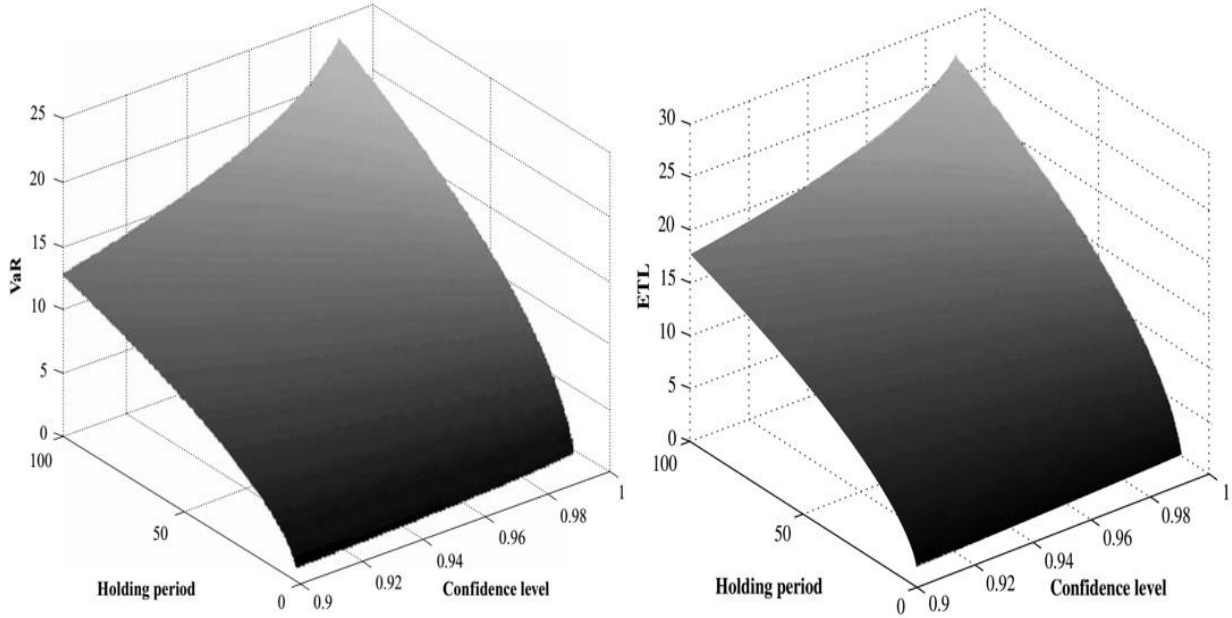


VaR measures the maximum expected loss if an extreme event i.e., 'tail,' *does not occur*, and the ETL measures expected loss *on average* if an extreme event i.e., 'tail,' *does occur*

In the real 'sociotechnical' world, **tails are the norm**! Hence, must account for tail risks.

http://ssrn.com/abstract=2553547

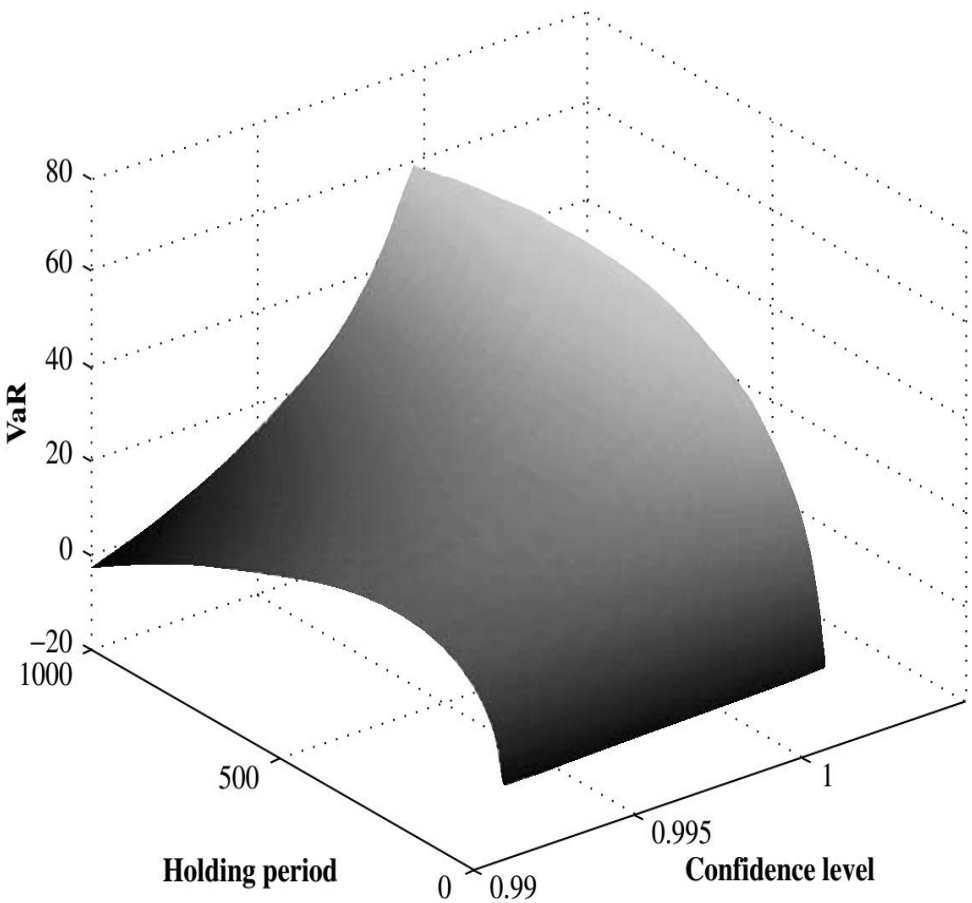
Comparison of How VaR and ETL vary with the Two Parameters



The actual loss (and related risk), however, could be more extreme than the average of the left tail risk. Hence, ETL does not provide any information about the severity of loss by which VaR is exceeded.

http://ssrn.com/abstract=2553547

Need for Extreme Value Methods… and Data



$$\Pr\left\{\frac{M_n - b_n}{a_n} \le x\right\} = F(a_n x + b_n)^n \to H(x)$$

$$H(x) = \exp(-e^{-x}), \text{ all } x \quad \text{(Gumbel)}$$

$$H(x) = \begin{cases} 0 & x < 0 \\ \exp(-x^{-\alpha}) & x > 0 \end{cases} \quad \text{(Fréchet)}$$

$$H(x) = \begin{cases} \exp(-|x|^{\alpha}) & x < 0 \\ 1 & x > 0 \end{cases} \quad \text{(Weibull)}$$

http://ssrn.com/abstract=2553547

Global Cyber Insurance Crisis Averted

Averted impending national Cyber risk & Cyber-insurance crisis.

- First known **Cyber-Finance-Trust**™ framework...
- First known model risk management framework...
- First known analysis establishing significant and extreme *model risks*, *tail risks*, and, *systemic risks*...
- Empirical study of VaR and Bayesian statistical inference methodologies for containing model risks...
- Markov Chain Monte Carlo Models, Gibbs Sampling and Metropolis-Hastings statistical computing algorithms...
- First known portfolio theory based framework for Cyber insurance modeling...
- Framework for enabling Knightian uncertainty management...

Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics http://ssrn.com/abstract=2553547

Materiality of Cyber Risk, Lack Thereof

- Data for cyber risk losses is sparse given negligible mention in SEC filings as compliance requirements leave reporting to individual firms' judgment about materiality.
- Loss data is underreported which can lead to specific and systemic underassessment of cyber risk by wide margin.
- McKinsey: $9Tn to $21Tn of economic-value creation is subject to cyber risk exposure in next 5 to 7 years'.
- Most large firms tend to not report them in public financial disclosures as they are deemed 'not material'.

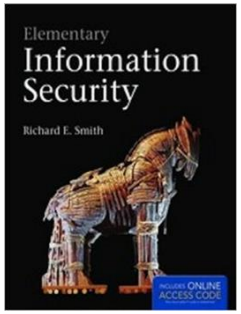
"Businesses inconsistently disclose cyber risk and incident information to investors today.
Many businesses infrequently and inconsistently account for cyber incidents and related losses.
There is inconsistent understanding and interpretation of the material cyber risk and incident disclosure standard."

https://www.sec.gov/comments/4-673/4673-11.pdf

Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics http://ssrn.com/abstract=2553547

The Cyber-Finance-Trust Framework

- *Unlike other risks, cyber risk poses a uniquely different set of exposures as it is intertwined with the medium and the message in the digital world of networked communications.*
- The *more significant and latent cyber risk is in the inherent and potential vulnerabilities* in the enabling *medium* such as the underlying operating system or networking software.
- *Vulnerabilities inherent in the medium can be exploited resulting in cyber risk regardless of user's actions.*



"In Cyber ***and*** Finance Trust Relationships... Every Entity a Plausible Target... Every Entity, Device, Network, Actor, or, Agent: A Potential 'Trojan Horse'..."

Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics http://ssrn.com/abstract=2553547

The Cyber-Finance-Trust Framework

The Trust Troika: Cyber-Finance-Trust™

- The Cyber-Finance-Trust Framework for Cyber Insurance
- Cyber *Games* and *Economic Value* Creation & Destruction
- In *Trust Relationships*, Every Entity a Plausible Target
- Financial Markets as *Scoreboards of Economic Value*
- Finance-Cyber Interact with No Cyber Risk Score in Filings
- Using VaR to Model Financial Risk and Cyber Risk
  - Such risk of failures of a model when it fails given that its underlying assumptions, boundaries, and limitations are not compatible with its application is called ***model risk***.

Quantitative Modeling of Trust and Trust Management Protocols in Next Generation Social Networks Based Wireless Mobile Ad Hoc Networks http://ssrn.com/abstract=2539180

Beyond Mis-measure of Cyber Risk

Cyber-Finance-Trust Framework for Cyber Risk Insurance Modeling

Cyber risk inherent in *all* cyber activities including cyber-finance,-economics.
Just like use of *any* model entails associated ***model risk***,
Similarly use of cyber activities entails associated ***cyber risk***.

Cyber risk is "risk affecting the ***confidentiality***, ***availability***, ***integrity***, ***authentication***, ***non-repudiation***, or ***accessibility*** of **information**."

"Unlike other risks, ***cyber risk*** poses a ***uniquely different set of exposures*** as it is ***intertwined with*** the **medium** and the **message** in the increasingly global **interconnected**, **distributed**, and, **networked** world of **digital communications** powered by **universal use** and **reuse** of enabling **global monocultures** of information and communication technologies and **standard computing network protocols**."

Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management
http://ssrn.com/abstract=2538401
Markov Chain Monte Carlo Models, Gibbs Sampling, & Metropolis Algorithm
http://ssrn.com/abstract=2553537

Beyond Mis-measure of Cyber Risk

Advancing Beyond Model Risk of VaR for Cyber Risk Loss Assessment

- Systemic, highly correlated, and interdependent nature of Cyber risks
- VaR not appropriate model given the 'systemic' nature of Cyber risks
- VaR doesn't satisfy '**subadditivity**' criterion of '**coherent risk measures**.'

Historical Simulation Based VaR: relies upon historical correlations;

MC based VaR: can use any statistical distribution (including normal), relies on several assumptions about specific statistical distributions chosen and extensive computing po $\sigma_p^2 = W^T \sum W$ cal computing $VaR_c = VaR_{1-\alpha} = P z_\alpha \sigma_p$

Parametric VaR: relies upon statistical **linearity** and **normality** assumptions;

$$\sum = \begin{pmatrix} \sigma_{11} & \sigma_{12} & \cdots & \sigma_{1n} \\ \sigma_{21} & \sigma_{22} & \vdots & \sigma_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{n1} & \sigma_{n2} & \vdots & \sigma_{nn} \end{pmatrix}$$

$$\min \sigma_p^2 = \min W^T \sum W \quad \text{s.t. } W^T R = r^*, \quad \sum_i^N w_i = 1 \quad w_i \geq 0$$

N (0, 1) "VaR is just one of multiple measures of risk we use to assess overall risk in the

[Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management](http://ssrn.com/abstract=2538401)
http://ssrn.com/abstract=2538401 http://ssrn.com/abstract=2594859

Beyond Mis-measure of Cyber Risk

Advancing Beyond Model Risk of VaR for Cyber Risk Loss Assessment

- Systemic, highly correlated, and interdependent nature of Cyber risks
- VaR not appropriate model given the 'systemic' nature of Cyber risks
- VaR doesn't satisfy '**subadditivity**' criterion of '**coherent risk measures**.'

Modified VaR: $\text{MSR} = \frac{R_P - R_F}{\text{MVaR}_{1-\alpha}}$ $\quad \text{MVaR}_c = \text{MVaR}_{1-\alpha} = \mu - z_{cf}\,\sigma_p$

$$z_{cf} \approx z_\alpha + (z_\alpha^2 - 1)\frac{S}{6} + (z_\alpha^3 - 3z_\alpha)\frac{K}{24} - (2z_\alpha^3 - 5z_\alpha)\frac{S^2}{36}$$

$$z_\alpha \approx N(0,1) \qquad E(z_\alpha) = 0 \qquad E(z_\alpha^2) = 1 \qquad E(z_\alpha^3) = 0 \qquad E(z_\alpha^4) = 3$$

$$S = \frac{n}{(n-1)(n-2)} \sum_{i=1}^{n} \left(\frac{x_i - \bar{x}}{s}\right)^3 \qquad K = \left[\frac{n(n+1)}{(n-1)(n-2)(n-3)} \sum_{i=1}^{n} \left(\frac{x_i - \bar{x}}{s}\right)^4\right] - \frac{3(n-1)^2}{(n-2)(n-3)}$$

Expected Shortfall (ES, ETL, T-VaR, CTE): http://ssrn.com/abstract=2594859

Subadditivity (diversification) $R(L_1 + L_2) \leq R(L_1) + R(L_2)$

Positive homogeneity (scaling) $R(\lambda L) = \lambda R(L)$, for every $\lambda > 0$

Monotonicity $R(L_1) < R(L_2)$ if $L_1 < L_2$

Transition property $R(L + a) < R(L) - a$

$$ES_\alpha \equiv \frac{1}{1-\alpha} \int_\alpha^1 VaR_c(L)\,dc$$

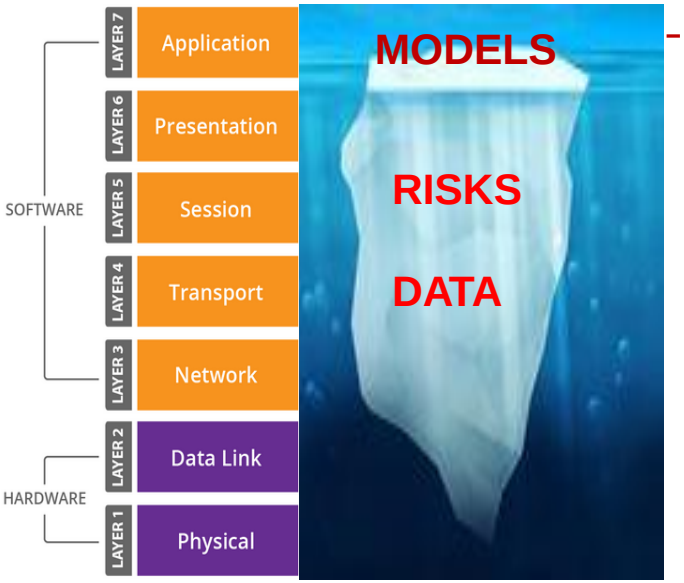
$$ES_{1-\alpha} = E[L | L > VaR_{1-\alpha}]$$

The 'Iceberg' of Cyber-Finance Risk

Cyber Finance: IT & Telco **networks** based finance of *post-WWW era* with products-services-processes, production-distribution-consumption channels digital, cyber, and virtual.

Given common and shared platforms, hardware, software, exchanges, and networks across many of the players in the Finance industry, there is a greater probability of correlated cyber risks.

http://ssrn.com/abstract=2590258



Increasing Knightian Uncertainty

Model Risk Management Critical

SSL/TLS, IPSec, PKI, Crypto

DATA: IN TRANSIT, IN USE, AT REST

TIME data SPACE

‘*Uncharted Territories*’ of Cyber-Finance

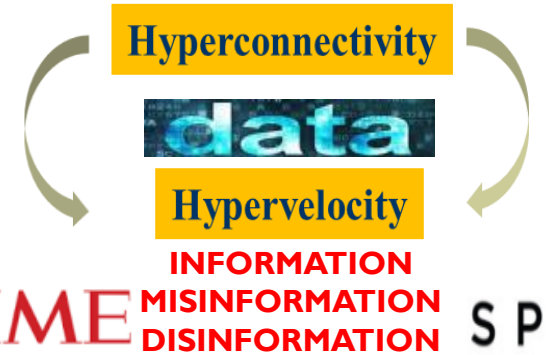
“As we know,
There are known knowns.
There are things we know we know.
We also know
There are **known unknowns***.
That is to say
We know there are some things
We do not know.
But there are also **unknown unknowns***,
The ones we don’t know

We don’t know.”

-- Donald Rumsfeld, US Secretary of Defense, Feb. 12, 2002

“That hasn’t happened before. It’s a brave new world. You are in **uncharted territory**....”

New York Times on the Financial Crisis



Cybersecurity & Cyber-Finance Risk Management: Strategies, Tactics, Operations, &, Intelligence: Understanding Vulnerabilities, Threats, & Risk Mitigation: http://ssrn.com/abstract=2693886

Beyond Risk to Managing Uncertainty

Risk, Uncertainty, and Profit for the Cyber Era: 'Knight Reconsidered'
http://ssrn.com/abstract=2553547

"Normality has been an accepted wisdom in economics and finance for a century or more. Yet in real-world systems, nothing could be less normal than normality. Tails should not be unexpected, for they are the rule… As the world becomes increasingly integrated – financially, economically, socially – interactions among the moving parts may make for potentially fatter tails. **Catastrophe risk may be on the rise.**"

-- Andrew G Haldane, Executive Director, Financial Stability and member of the Financial Policy Committee and Benjamin Nelson, Economist, Financial Stability, Bank of England, in 'Tails of the unexpected' speech at "The Credit Crisis Five Years On: Unpacking the Crisis", 8 June 2012.

Beyond NHST-Determinism to Bayesian

http://www.amstat.org/newsroom/pressreleases/P-ValueStatement.pdf

March 07, 2016

Scientific method: Statistical errors : Nature News & Comment, **Nature, 12 February 2014**
http://www.nature.com/news/scientific-method-statistical-errors-1.14700

Statistics: P values are just the tip of the iceberg, **Nature, 28 April 2015**
http://www.nature.com/news/statistics-p-values-are-just-the-tip-of-the-iceberg-1.17412

How scientists fool themselves – and how they can stop, **Nature, 07 October 2015**
http://www.nature.com/news/how-scientists-fool-themselves-and-how-they-can-stop-1.18517

Statisticians issue warning over misuse of *P* values, **Nature, 07 March 2016**
http://www.nature.com/news/statisticians-issue-warning-over-misuse-of-p-values-1.19503

Psychology journal bans *P* values, **Nature, 26 February 2015**
http://www.nature.com/news/psychology-journal-bans-p-values-1.17001

The fickle *P* value generates irreproducible results, **Nature, 26 February 2015**
http://www.nature.com/nmeth/journal/v12/n3/full/nmeth.3288.html

"The p-value was never intended to be a substitute for **scientific reasoning**," said Ron Wasserstein, the ASA's executive director. "**Well-reasoned** statistical **arguments** contain much more than the value of a single number and whether that number exceeds an arbitrary threshold. The ASA statement is intended to steer research into a 'post p0.05' era."

Beyond Model Risk Management to Model Risk Arbitrage for Fintech Era: How to Navigate 'Uncertainty'...When 'Models' are 'Wrong'...And 'Knowledge'...'Imperfect'! http://ssrn.com/abstract=2766099

Beyond NHST-Determinism to Bayesian

NCBI Resources How To

PMC US National Library of Medicine National Institutes of Health

PMC Limits Advanced Journal list

Journal List › PLoS Med › v.2(8); 2005 Aug › PMC1182327

PLOS | MEDICINE A Peer-Reviewed, Open Access Journal

View this Article | Submit to PLOS | Get E-Mail Alerts | Contact Us

PLoS Med. 2005 Aug; 2(8): e124. PMCID: PMC11823

Published online 2005 Aug 30. doi: 10.1371/journal.pmed.0020124

Why Most Published Research Findings Are False

John P. A. Ioannidis

Author information ▶ Copyright and License information ▶

See "Minimizing Mistakes and Embracing Uncertainty", e272.
See "Truth, Probability, and Frameworks" in volume 2, e361.
See "Power, Reliability, and Heterogeneous Results" in volume 2, e386.
See "The Clinical Interpretation of Research" in volume 2, e395.
See "Author's Reply" in volume 2, e398.
See "Why Most Published Research Findings Are False: Problems in the Analysis" in volume 4, e168.
See "Why Most Published Research Findings Are False: Author's Reply to Goodman and Greenland" in volume 4, e215.
See "Why Current Publication Practices May Distort Science" in volume 5, e201.

This article has been cited by other articles in PMC.

PLoS Med

Stanford MEDICINE | News Center

http://jama.jamanetwork.com/article.aspx?articleid=201218

JAMA The Journal of the American Medical Association

FRONT PAGE ALL NEWS TOPICS MULTIMEDIA

Email Share 154 Tweet

Search News... Go

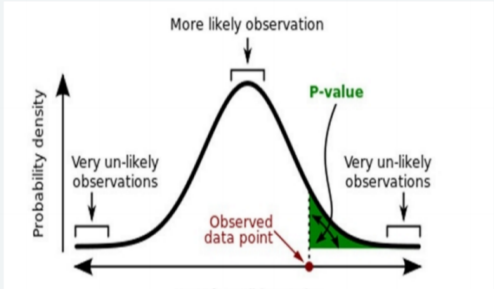
Misleading p-values showing up more often in biomedical journal articles

A review of p-values in the biomedical literature from 1990 to 2015 shows that these widely misunderstood statistics are being used increasingly, instead of better metrics of effect size or uncertainty.

MAR 15 2016

A study of millions of journal articles shows that their authors are increasingly reporting p-values but are often doing so in a misleading way, according to a study by researchers at the Stanford University School of Medicine. P-values are a measure of statistical significance intended to inform scientific conclusions.

Because p-values are so often misapplied, their increased use probably doesn't indicate an



RELATED NEWS

Re-analysis of clinical trial data can change conclusions, say researchers

A re-analysis of raw data from published clinical trials

Sep 9, 2014

Stanford launches center to strengthen quality of scientific research worldwide

MEDIA CONTACTS

JENNIE DUSHECK
Tel 650-725-5376
dusheck@stanford.edu

MARGARITA GALLARDO
Tel 650-723-7897
mjgallardo@stanford.edu

LEADING IN PRECISION HEALTH

http://www.amstat.org/newsroom/pressreleases/P-ValueStatement.pdf

March 07, 2016

MODEL RISKS OF 'NORMAL SCIENCE'

ASA News

AMERICAN STATISTICAL ASSOCIATION
Promoting the Practice and Profession of Statistics®

732 North Washington Street, Alexandria, VA 22314 • (703) 684-1221 • Toll Free: (888) 231-3473 • www.amstat.org • www.twitter.com/AmstatNews

AMERICAN STATISTICAL ASSOCIATION RELEASES STATEMENT ON STATISTICAL SIGNIFICANCE AND *P*-VALUES

Provides Principles to Improve the Conduct and Interpretation of Quantitative Science

March 7, 2016

Bayesian & Markov Chain Monte Carlo

Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management:

$$p(x) = \sum_y \quad p(x,y) \qquad\qquad p(x) = \int_y dy \; p(x,y)$$

$$p(y|\boldsymbol{x}) = \frac{p(y,x)}{\sum_y \; p(y,x)} = \frac{p(y,x)}{p(\boldsymbol{x})} \;, \quad p(x|y) = \frac{p(x,y)}{\sum_x \; p(x,y)} = \frac{p(x,y)}{p(y)}$$ given discrete x and y,

$$p(y|x) = \frac{p(y,x)}{\int_y \; dy \, p(y,x)} = \frac{p(y,x)}{p(x)} \;, \quad p(x|y) = \frac{p(x,y)}{\int_x \; dx \; p(x,y)} = \frac{p(x,y)}{p(y)}$$ given continuous x and y

$$\boldsymbol{p(y|x)} = \frac{\boldsymbol{p(x\,|\,y)p(y)}}{\sum_{\boldsymbol{y}} \boldsymbol{p(x,y)}} \Leftrightarrow \frac{p(x\,|\,y)p(y)}{\int_y \; dy \; p(x,y)} \qquad \boldsymbol{p(\theta_j\,|\,D_i)} = \frac{p(\theta_j, D_i)}{p(D_i)} = \frac{\boldsymbol{p(D_i\,|\,\theta_j)\,p(\theta_j)}}{\boldsymbol{p(D_i)}}$$

$$p(D_i\,|\,\theta_j) = \frac{p(D_i,\theta_j)}{p(\theta_j)} = \frac{p(\theta_j\,|\,D_i)\,p(D_i)}{p(\theta_j)} = \frac{p(\theta_j\,|\,D_i)\,p(D_i)}{\sum_i \; p(\theta_j\,|\,D_i)\,p(D_i)}$$

[Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management](http://ssrn.com/abstract=2538401)
http://ssrn.com/abstract=2538401

Bayesian & Markov Chain Monte Carlo

Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management:

$$p(\theta_j \mid D_i) = \frac{p(D_i \mid \theta_j)\, p(\theta_j)}{p(D_i)} \quad \text{i.e.} \quad Posterior = \frac{Likelihood * Prior}{Evidence}$$

$$p(D_i) = \sum_\theta p(D_i, \theta_j) = \int_\theta d\theta \; p(D_i \mid \theta_j)\; p(\theta_j) \qquad p(\theta_j \mid D_i, M) = \frac{p(D_i \mid \theta_j,\; M)\, p(\theta_j \mid M)}{p(D_i \mid M)}$$

$$p(M_1 \mid D_i) = p(M_1, D_i) \,/\, p(D_i) = p(D_i \mid M_1)\, p(M_1) \,/\, p(D_i)$$

$$p(M_2 \mid D_i) = p(M_2, D_i) \,/\, p(D_i) = p(D_i \mid M_2)\, p(M_2) \,/\, p(D_i)$$

$$\frac{p(M_1 \mid D_i)}{p(M_2 \mid D_i)} = \frac{p(D_i \mid M_1)\, p(M_1)}{p(D_i \mid M_2)\;\; p(M_2)}$$

Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management
http://ssrn.com/abstract=2538401

Bayesian & Markov Chain Monte Carlo

"This reliance on models to handle risk carries its own risks."

Markov Chain Monte Carlo Models, Gibbs Sampling & Metropolis Algorithm for High-Dimensionality Complex Stochastic Problems. (Malhotra 2014)

Bayesian inference for doing high dimension parameter space analyses

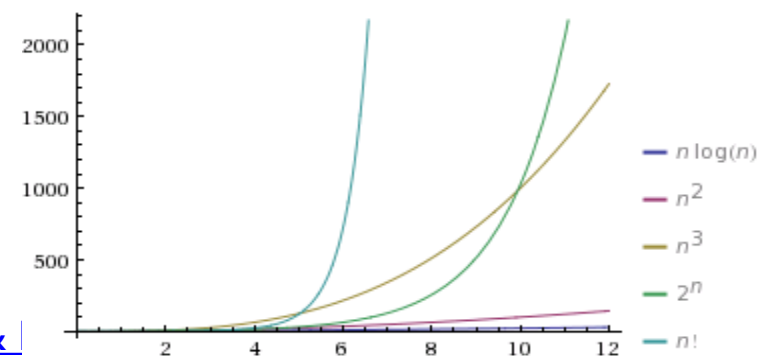
- Feasible with Markov Chain Monte Carlo statistical computing algorithms
- Metropolis Hastings algorithm and Gibbs Sampling algorithm

MCMC: A common general quantitative method to find approximate solutions to computationally complex problems in *polynomial time*…

Polynomial Time $O(n^k)$ s.t. $k > 1$

Exponential Time $O(k^n)$ s.t. $k > 1$

n = length of input



Markov Chain Monte Carlo Models, Gibbs Sampling, &
http://ssrn.com/abstract=2553537

Bayesian & Markov Chain Monte Carlo

Markov Chain Monte Carlo Models, Gibbs Sampling & Metropolis Algorithm for High-Dimensionality Complex Stochastic Problems.

Monte Carlo integration $\int_a^b h(x)dx = \int_a^b f(x)\,p(x)dx = E_{p(x)}\,[f(x)] \approx \frac{1}{n}\sum_{i=1}^{n} f(x_i)$

$I(y) = \int f(y|x)p(x)dx \approx \frac{1}{n}\sum_{i=1}^{n} f(y|x_i)$

Gibbs Sampling: Generating random variables from a marginal distribution indirectly without the need for calculating the distribution density.

-E.g. Solve complex multivariate stochastic model with N parameters (i.e. N-Dim.) using N univariate (i.e., one-dimensional) conditional distributions.

$\mathcal{L}(\theta|X) = P(X|\theta)$ $\qquad f_i\ (\theta_i|\theta_{j\neq i},\ X,\ M)$

$f_1\ (\theta_1|\theta_2, \theta_3, X, M)$ random sample from $f_1\ (\theta_1|\ \theta_{2,0}, \theta_{3,0}, X, M)$ random draw as $\theta_{1,1}$

$f_2\ (\theta_2|\theta_3, \theta_1, X, M)$ random sample from $f_2\ (\theta_2|\ \theta_{3,0}, \theta_{1,1}, X, M)$ random draw as $\theta_{2,1}$

$f_3\ (\theta_3|\theta_1, \theta_2, X, M)$ random sample from $f_3\ (\theta_3|\ \theta_{1,1}, \theta_{2,1}, X, M)$ random draw as $\theta_{3,1}$

$\theta_{1,0}, \theta_{2,0}, \theta_{3,0} \rightarrow \theta_{1,1}, \theta_{2,1}, \theta_{3,1} \rightarrow \theta_{1,2}, \theta_{2,2}, \theta_{3,2} \rightarrow \ldots \rightarrow \theta_{1,m}, \theta_{2,m}, \theta_{3,m}$

Markov Chain Monte Carlo Models, Gibbs Sampling, & Metropolis Algorithm
http://ssrn.com/abstract=2553537

Bayesian & Markov Chain Monte Carlo

Dropping the burn-in sample of first m draws $\theta_{1,m}, \theta_{2,m}, \theta_{3,m}$

Gibbs sample: $(\theta_{1,m+1}, \theta_{2,m+1}, \theta_{3,m+1}), \ldots, (\theta_{1,n}, \theta_{2,n}, \theta_{3,n})$

random sample from the joint distribution $f(\theta_1, \theta_2, \theta_3 | X, M)$

Metropolis Algorithm :

$p(\theta|X) = f(\theta|X)/K$ (where K is the normalizing constant)

Start with a random draw of some initial value θ_o: $f(\theta_o|X) > 0$

Given previous draw θ_{t-1} for the tth iteration, draw a candidate sample θ_* *jumping distribution* $J_t(\theta_t|\theta_{t-1})$

$r = p(\theta_*|X) / p(\theta_{t-1}|X) = f(\theta_*|X) / f(\theta_{t-1}|X)$ $\quad J_t(\theta_i|\theta_j) = J_t(\theta_j|\theta_i)$ for all θ_i, θ_j, and t

$r > 1$ accept the candidate point θ_* as θ_t, i.e., set $\theta_t = \theta_*$ draw a candidate sample

$r < 1$ accept the candidate and set $\theta_t = \theta_*$ with probability r
else reject it, i.e. set $\theta_t = \theta_{t-1}$ draw a candidate sample

computing the acceptance probability of candidate $r = \min[f(\theta_*|X) / f(\theta_{t-1}|X), 1]$

$p_{move} = \min[\mathcal{P}(\theta_{proposed}) / \mathcal{P}(\theta_{current}), 1]$

➡ Markov chain $(\theta_0, \theta_1, \ldots, \theta_k, \ldots)$ ➡ burn-in period prior m of n steps ➡ $(\theta_{m+1}, \ldots, \theta_n)$

Markov Chain Monte Carlo Models, Gibbs Sampling, & Metropolis Algorithm
http://ssrn.com/abstract=2553537

Bayesian & Markov Chain Monte Carlo

Metropolis-Hastings Algorithm : arbitrary transition probability function $J_t(\theta_i|\theta_j) = \Pr(\theta_i \rightarrow \theta_j)$

density at the candidate point θ_* and at the current point θ_{t-1}:

$$r = (f(\theta_*|X) / J_t(\theta_*|\theta_{t-1})) / (f(\theta_{t-1}|X) / J_t(\theta_{t-1}|\theta_*)) = (f(\theta_*|X)\ J_t(\theta_{t-1}|\theta_*)) / (f(\theta_{t-1}|X)\ J_t(\theta_*|\theta_{t-1}))$$

acceptance probability of the candidate point

$$r = \min[(f(\theta_*|X) / J_t(\theta_*|\theta_{t-1})) / (f(\theta_{t-1}|X) / J_t(\theta_{t-1}|\theta_*)), 1] = \min[(f(\theta_*|X)\ J_t(\theta_{t-1}|\theta_*)) / (f(\theta_{t-1}|X)\ J_t(\theta_*|\theta_{t-1})), 1]$$

Metropolis-Hastings Algorithm = Metropolis Algorithm when $J_t(\theta_i|\theta_j) = J_t(\theta_j|\theta_i)$

Markov Chain Monte Carlo Models, Gibbs Sampling, & Metropolis Algorithm for High-Dimensionality Complex Stochastic Problems:
Applications in Network and Computer Security http://ssrn.com/abstract=2553537

Increasingly Vulnerable Time and Space

Los Angeles Times

NATION

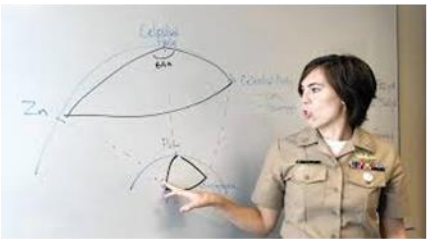
In the era of GPS, Naval Academy revives celestial navigation

[Beyond Model Risk Management to Model Risk Arbitrage for Fintech Era: How to Navigate 'Uncertainty'...When 'Models' are 'Wrong'...And 'Knowledge'...'Imperfect'! http://ssrn.com/abstract=2766099](http://ssrn.com/abstract=2766099)

Naval Academy reinstates celestial navigation

MilitaryTimes

12:20 p.m. EST November 2, 2015



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES

Recent Vulnerabilities

January 2016 NTP-4.2.8p6 Security Vulnerability Announcement (Medium)

NTF's NTP Project has been notified of the following low- and medium-severity vulnerabilities that are fixed in ntp-4.2.8p6,

- Bug 2948 / CVE-2015-8158: Potential Infinite Loop in `ntpq`
  - Reported by Cisco ASIG
- Bug 2945 / CVE-2015-8138: origin: Zero Origin Timestamp Bypass
  - Reported by Cisco ASIG
- Bug 2942 / CVE-2015-7979: Off-path Denial of Service (DoS) attack on authenticated broadcast mode
  - Reported by Cisco ASIG
- Bug 2940 / CVE-2015-7978: Stack exhaustion in recursive traversal of restriction list
  - Reported by Cisco ASIG
- Bug 2939 / CVE-2015-7977: `reslist` NULL pointer dereference

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELAT

Vulnerabilities Identified in Network Time Protocol Daemon (ntpd)

Original release date: October 21, 2015 | Last revised: October 22, 2015

Print | Tweet | Send | Share

TIME

SPACE

Increasingly Vulnerable Time and Space

RISK ASSESSMENT / SECURITY & HACKTIVISM

New attacks on Network Time Protocol can defeat HTTPS and create chaos

Exploits can be used to snoop on encrypted traffic and cause debilitating outages.

by **Dan Goodin** - Oct 21, 2015 6:07pm EDT

Serious weaknesses in the Internet's time-synchronization mechanism can be exploited to cause debilitating outages, snoop on encrypted communications, or tamper with Bitcoin transactions, computer scientists warned Wednesday.

The vulnerabilities reside in the Network Time Protocol, the widely used specification computers use to ensure their internal clocks are accurate. Surprisingly, connections between computers and NTP servers are rarely encrypted, making it possible for hackers to perform man-in-the-middle attacks that reset clocks to times that are months or even years in the past. In a paper published Wednesday titled *Attacking the Network Time Protocol*, the researchers described several techniques to bypass measures designed to prevent such drastic time shifts. The paper also described ways to prevent large numbers of computers from successfully connecting to synchronization servers.

The attacks could be used by malicious actors to wreak havoc on the Internet. An attack that prevented sensitive computers and servers from receiving regular time-synchronization updates could cause malfunctions on a mass scale. In many cases, such denial-of-service hacks can be carried out even when attackers are "off-path," meaning the hacker need not have the ability to monitor traffic passing between a computer and NTP server.

TIME

SPACE

Going back in time

Even worse, the attacks can be used to snoop on encrypted traffic or to bypass important security measures such as DNSSEC specification preventing the tampering of domain name system records. The most troubling scenario involves bypassing HTTPS encryption by forcing a computer to accept an expired transport layer security certificate.

http://ssrn.com/abstract=2766099

Vulnerable Digital & Crypto-Currencies

'Known' Vulnerabilities: Block Chain & Crypto-Currencies

http://ssrn.com/abstract=2766099

Known and Potential Attacks and Vulnerabilities of Bitcoin

Pros and cons of Bitcoin as well as potential weaknesses in its security and encryption protocols were discussed above; other potential vulnerabilities are summarized below. Most probably, the pseudonymous Bitcoin inventor didn't envision today's global BTC mining computational arms-race with armies of botnets using global captive computers, software vendors using malware to steal customers' CPU power for mining BTCs, or clearly illegal service using ransom-ware forcing law enforcement officers into making BTC payments via their openly public customer service Web site.

Bitcoin is known for its [pseudo-]anonymity of user identification as it uses randomly generated public keys for Bitcoin addresses; however, it is not truly anonymous. As noted in the US Senate Hearing testimony of the Criminal Division: "Criminals are drawn to services that allow users to conduct financial transactions while remaining largely anonymous... [However,] To be clear, virtual currency is not necessarily synonymous with anonymity." Public key addresses are self-identified by users for receiving payments or when they need to convert BTCs to other currencies including real money when user identity is linked with related public key address. Furthermore, different public keys that are input in a specific transaction or a se ding payments need to l 'change' from Bitcoin transactions can be linked to respective input addresses as well as input users. Private transactions between parties of same exchange are privy to the exchange which may be able to bypass such identification by not using the strict Bitcoin protocol of transparency of each transaction. The 'default' Bitcoin protocol doesn't provide *true* anonymity which may require protection from both *forward attacks* and *reverse attacks*. Forward attacks involve getting something that identifies a user using coins received with methods that should remain secret. Reverse attacks involve getting something that should remain secret by using coins that can identify a user.

http://yogeshmalhotra.com/BitcoinProtocol.html

Several additional 'weaknesses' representing vulnerability of Bitcoin coins and transactions are identified next. Wallet files are vulnerable to theft and need to be encrypted and backed off-line. Old backup wallet files and contents can be retrieved with existing backup facilities. Coin's history can be traced to link user identities to the pseudo-anonymous addresses. Unlike Bitcoin addresses, if a payment is sent to IP address, man-in-the-middle attack is feasible given IP addresses can be spoofed. Unless node-to-node encryption is used, packet sniffing can reveal the sent transactions. Distributed denial of service (DDoS) attacks pose potential threats just like with any other networked cryptographic service. However, deep-pocketed DDoS attacks using 'remarkable 100 G/bits per second in bandwidth' and million-dollar hacking heists are becoming increasingly common. *Timejacking* attacks can be done by announcing inaccurate timestamps when altering the node's networ computational res efficient mining gear only raises the network 'difficulty' without reducing energy use and cheaper energy linearly increases mining energy use. Similar concerns apply to other cryptographic proof of work currencies such as Litecoin as well.

http://yogeshmalhotra.com/Future_of_Bitcoin.html

Besides vulnerabilities of encryption protocols to available ***quantum*** computers, *classical* computers capable of 54.9-petaflops may pose major '>50%' threat to Bitcoin. The specific attack results from anyone in the network acquiring more than 50% computing power being able to exclude, modify, and self-reverse transactions and prevent some or all 'mining'

Mt. Gox Creditors Seek More Than $22 Billion

Almost Half a Billion of Bitcoins Vanishes - WSJ

Bitcoin, up 152%, tops $1 billion in total value

TIME

SPACE

Vulnerable Digital & Crypto-Currencies

Kaspersky and INTERPOL Say Blockchain is Vulnerable

http://ssrn.com/abstract=2766099

By Scott Fargo | Apr 11, 2015 9:00 AM EDT

14 18 16

Kaspersky Labs and INTERPOL have presented research in which they show how blockchain-based cryptocurrencies can potentially be abused with arbitrary data that can be disseminated through its public decentralized databases.

The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide

16 Feb 2015
Virus News

Kaspersky Lab, INTERPOL, Europol and authorities from different countries have combined efforts to uncover the criminal plot behind an unprecedented cyberrobbery. Up to one billion American dollars was stolen in about two years from financial institutions worldwide. The experts report that responsibility for the robbery rests with a multinational gang of cybercriminals from Russia, Ukraine and other parts of Europe, as well as from China. The Carbanak criminal gang responsible for the cyberrobbery used techniques drawn from the arsenal of targeted attacks. The plot marks the beginning of a new stage in the evolution of cybercriminal activity, where malicious users steal money directly from banks, and avoid targeting end users.

Since 2013, the criminals have attempted to attack up to 100 banks, e-payment systems and other financial institutions in around 30 countries. The attacks remain active. According to Kaspersky Lab data, the Carbanak targets included financial organizations in Russia, USA, Germany, China, Ukraine, Canada, Hong Kong, Taiwan, Romania, France, Spain, Norway, India, the UK, Poland, Pakistan, Nepal, Morocco, Iceland, Ireland, Czech Republic, Switzerland, Brazil, Bulgaria, and Australia.

It is estimated that the largest sums were grabbed by hacking into banks and stealing up to ten million dollars in each raid. On average, each bank robbery took between two and four months, from infecting the first computer at the bank's corporate network to making off with the stolen money.

The cybercriminals began by gaining entry into an employee's computer through spear phishing, infecting the victim with the Carbanak malware. They were then able to jump into the internal network and track down administrators' computers for video surveillance. This allowed them to see and record everything that happened on the screens of staff who serviced the cash transfer systems. In this way the fraudsters got to know every last detail of the bank clerks' work and were able to mimic staff activity in order to transfer money and cash out.

The billion-dollar advanced persistent threat is in your bank's network, if:

There are
files with .bin extension
at the following location:
\All users\%AppData%\Mozilla\
or c:\ProgramData\Mozilla\

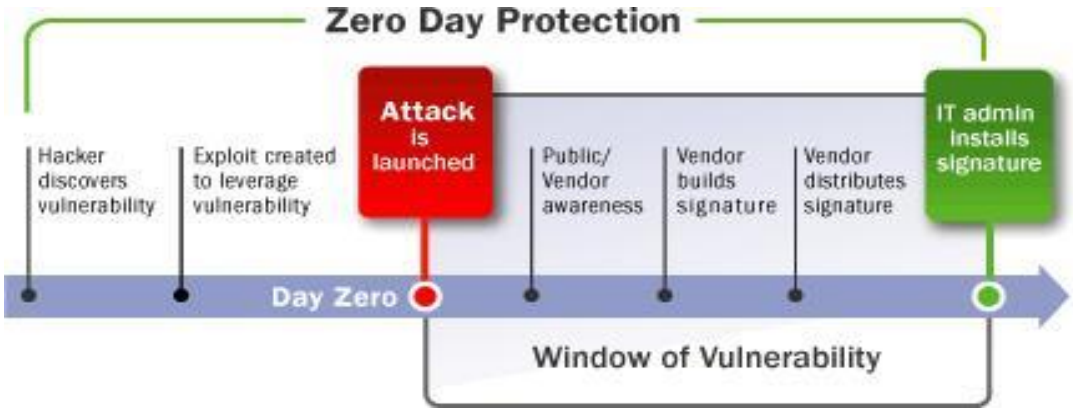
There is
a svchost.exe file
in Windows\System32\com\ catalogue
(or Windows\Syswow64\com\ catalogue - for 64-bit OS Windows)

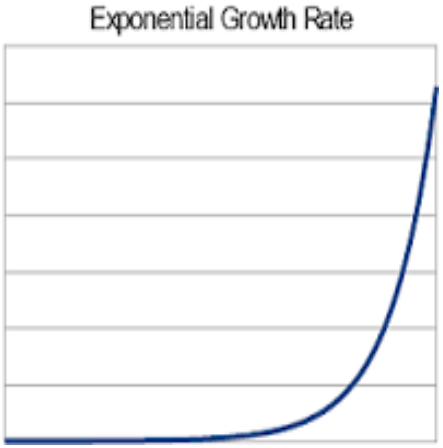
Among the active Windows services
the Services ending in "sys"
were found, duplicating a similar service stored without the "sys"
Example: you find an instance of the aspnetsys service while the legal aspnet service is active on the system.

Exponentially Growing Vulnerabilities

CVE, a key cybersecurity resource, is at risk inside and out

By Sean Sposito | March 25, 2016 | Updated: March 25, 2016 7:50pm





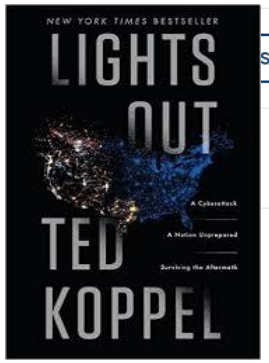
"Catastrophic" is the right word. On the scale of 1 to 10, this is an 11."

TIME SPACE

Beyond Model Risk Management to Model Risk Arbitrage for Fintech Era: How to Navigate 'Uncertainty'…When 'Models' are 'Wrong'…And 'Knowledge'…'Imperfect'! http://ssrn.com/abstract=2766099

Black Hat Finance of FinTech Models

http://ssrn.com/abstract=2766099



Lights Out:
A Cyberattack,
A Nation
Unprepared,
Surviving the
Aftermath

SCRIBE

SCIENTIFIC AMERICAN™

English Cart 0 Sign In |

THE SCIENCES MIND HEALTH TECH SUSTAINABILITY EDUCATION VIDEO PODCASTS BLOGS STORE

COMPUTING

The Most Vulnerable Ransomware Targets Are the Institutions We Rely On Most

Many vital public institutions such as hospitals and fire stations lack cybersecurity to ward off popular malware

By Annie Sneed on March 23, 2016

TIME

SPACE

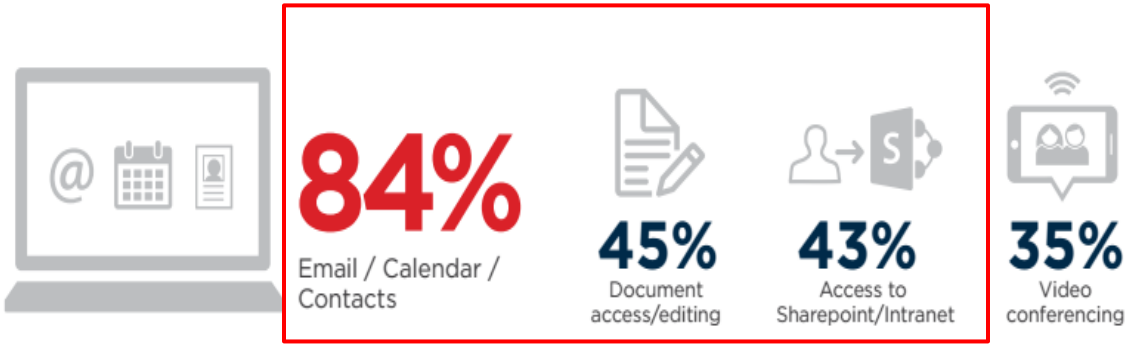
Black Hat Finance of FinTech Models

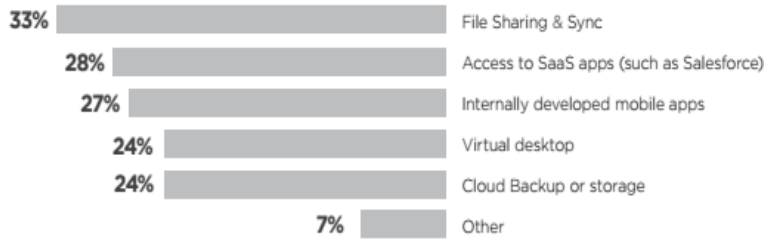
The Haunting Reality of Mobile Security Infographic Sources http://ssrn.com/abstract=2766099

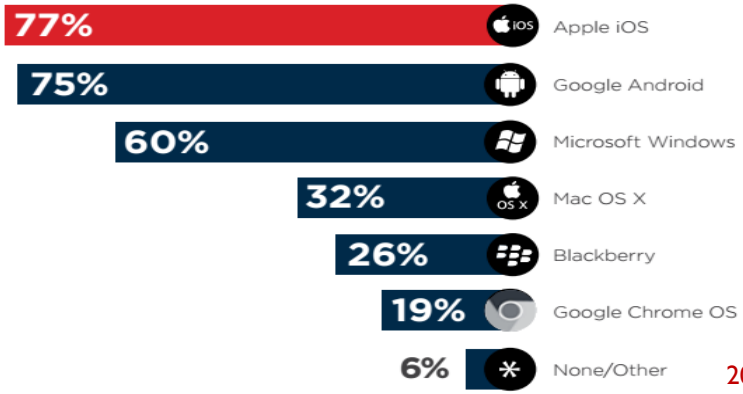
- **1,023,108,267** records breached in 2014. (Breach Level Index)
- **5.2 million** lost or stolen smartphones in the U.S. in 2014. (**Consumer Reports**)
- 44% of web attacks were launched from the U.S. and Germany. (Kaspersky Lab)
- **#1** weakest security link for businesses: mobile devices. (CyberEdge Group)
- **1-in-5** Android users experienced a mobile threat in 2014. (Kaspersky Lab)
- **Average U.S. Enterprise Cost of Cybercrime by Industry:** (Ponemon Institute)
  - **$8.6 million** for U.S. retail stores
  - **$12.7 million** in communications
  - **$14.5 million** in technology
  - **$20.8 million** in financial services

- **75%** or more mobile apps would fail basic security tests. (Gartner)
- **9X** more mobile banking Trojan attacks in 2014. (Kaspersky Lab)
- **56%** of enterprises admit to being unlikely they will detect a sophisticated threat. (EY)
- **37%** admitted that their enterprise has no real-time visibility on cyberattacks. (EY)

Black Hat Finance of FinTech Models







2016 BYOD & MOBILE SECURITY REPORT

TIME SPACE

Assume Breach & Crypto-Apocalypse

Number Field Sieve Cryptanalysis Algorithms for Most Efficient Prime Factorization on Composites
http://ssrn.com/abstract=2553544

Cybersecurity & Cyber-Finance Risk Management: Strategies, Tactics, Operations, &, Intelligence: Enterprise Risk Management to Model Risk Management: Understanding Vulnerabilities, Threats, & Risk Mitigation
http://ssrn.com/abstract=2693886

Trust is at the breaking point: The idea of a Cryptoapocapyse is far from science fiction. Heartbleed was just a taste of what this could look like. Could a website be trusted? How many keys were compromised? Could an organization be trusted online? The era of cloud computing, parallel processing, and GPUs are being used to test these attacks. The cost to compromise a MD5-signed digital certificate is now $0.65[17] in Amazon AWS, down from $200,000 in less than two years.[18]

MOST ALARMING THREATS (IN ORDER OF CONCERN)

1. WEAK CRYPTOGRAPHIC EXPLOIT
2. MOBILE CERTIFICATE MISUSE
3. CODE-SIGNING CERTIFICATE MISUSE
4. MALICIOUS MITM CERTIFICATES
5. SSH KEY MISUSE
6. SERVER CERTIFICATE MISUSE

2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point, Ponemon Institute, 2015.

Assume Breach & Crypto-Apocalypse

	Description of Attack Type	Example of Real-world Attack
Server Certificate Misuse	To impersonate public websites and decrypt encrypted traffic, attackers steal keys and certificates.	The theft of data on 4.5M healthcare patients in 2014 started with the exploit of Heartbleed to steal an SSL/TLS key and certificate that encrypted sensitive data.[4]
Code-signing Certificate Misuse	Attackers digitally sign malicious code to have it trusted and run.	The $1B theft by Carbanak operators was enabled by signed malware that looked like trusted software.[5]
SSH Key Misuse	Bad guys seeking to gain access to the most sensitive systems and data compromise SSH credentials.	APT operators like The Mask stole SSH keys and used their privileged access to compromise networks for over seven years.[6]
Man-in-the-middle (MITM) Attack	Cybercriminals compromise Certificate Authorities (CAs) or forge new certificates to trick users and monitor communications.	APT operators like Dark Hotel used a malicious CA and website certificates to get in and target executive communications.[7]
Weak Cryptographic Exploit	Adversaries target weak cryptography to create trusted keys and certificates.	As part of the Flame malware, Microsoft's software update service was spoofed by exploiting MD5-based signatures.[8]
Enterprise Mobility Certificate Misuse	Misuse of these credentials provides access to WiFi, VPN, or data protected by MDM/EMM systems.	An emerging threat that security professionals believe needs to be watched closely.

http://ssrn.com/abstract=2553544

"The Ponemon Institute's 2015 *Cost of Failed Trust* Report reveals most organizations believe the trust established by cryptographic keys and digital certificates, which they require for their businesses to operate, is in jeopardy…"

Cybersecurity & Cyber-Finance Risk Management: Strategies, Tactics, Operations, &, Intelligence: Understanding Vulnerabilities, Threats, & Risk Mitigation: http://ssrn.com/abstract=2693886

Healthcare: More Vulnerable than Finance?

- More than **90%** of healthcare organizations had a data breach.
- "The value of personal financial and health records is two or three times [the value of financial information alone], because there's so many more opportunities for fraud…"

  - Pittsburgh Post-Gazette, March 2015
- "Cyber criminals are selling the information on the black market at a rate of **$50 for each partial EHR**, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft."

  - FBI Bulletin, April 2014

Cybersecurity & Cyber-Finance Risk Management: Strategies, Tactics, Operations, &, Intelligence: Understanding Vulnerabilities, Threats, & Risk Mitigation: http://ssrn.com/abstract=2693886

Healthcare: More Vulnerable than Finance?

Kansas Heart Hospital hit with ransomware; attackers demand two ransoms

NETWORKWORLD

Hospital pays ransomware, but doesn't get files decrypted

By Ryan Whitwam on May 25, 2016 at 4:46 pm | 32 Comments

EXTREMETECH

Alert (TA16-091A)

Ransomware and Recent Variants

Original release date: March 31, 2016 | Last revised: May 06, 2016

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

U.S., Canada issue ransomware warning for hospitals after three hit in a week

By Joseph Conn | April 4, 2016

Modern Healthcare

22 **Hospital Declares 'Internal State of Emergency' After Ransomware Infection**

KrebsonSecurity

In-depth security news and investigation

Two more healthcare networks caught up in outbreak of hospital ransomware

New server-targeting malware hitting healthcare targets with unpatched websites.

ars technica

TECH APR 23 2016, 6:06 AM ET

Big Paydays Force Hospitals to Prepare for Ransomware Attacks

NBC NEWS

KIM ZETTER | SECURITY 03.30.16 1:31 PM

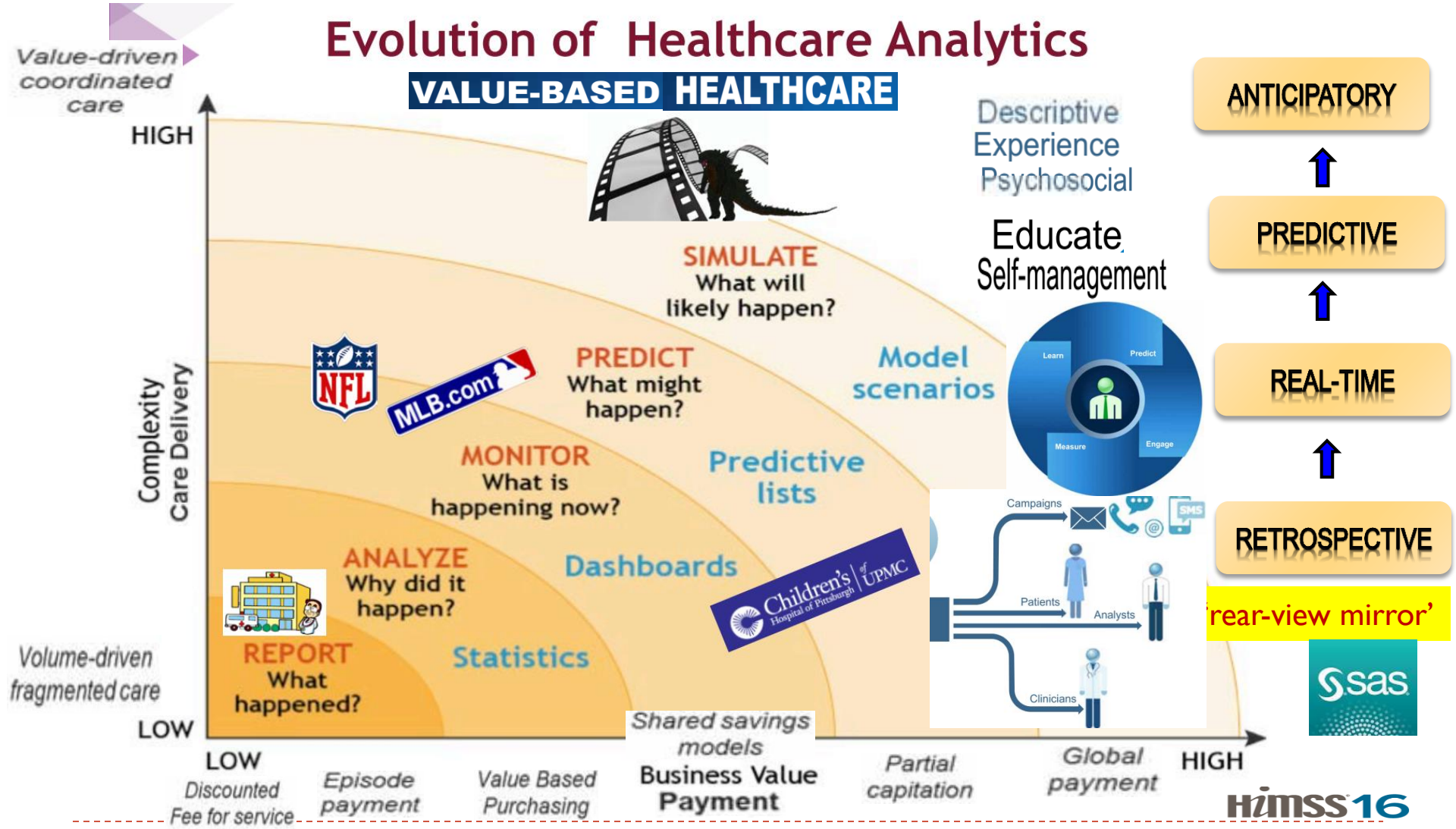
WHY HOSPITALS ARE THE PERFECT TARGETS FOR RANSOMWARE

WIRED

Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers

CSO

Healthcare Analytics: Following Finance Analytics?



Healthcare Analytics: Following Finance Analytics?

POPULATION HEALTH | WHAT IS IT? continuum of health and well-being through participation of, engagement with and targeted interventions for the population

ADVANCED ANALYTICS | USING MULTIPLE METHODS

SOURCE DATA: Social, Biometric, Economic, Hospitals, Claims, Pharmacy

For known patterns	For unknown patterns	For complex patterns	For unstructured data	For optimizing
Rules	**Anomaly Detection**	**Predictive Models**	**Text Mining**	**Simulation & Optimization**
Rules to surface known issues	Algorithms to surface unusual (out-of-band) behaviors	Identify patterns and event relationships to indicate potential future events	Leverage unstructured data elements in analytics	Simulate scenarios of care models, financial and other constraints; optimize actions
Examples: • Relevant diagnosis code recorded • Prescription not filled	Examples: • New symptom presents • # patients with event exceeds expected	Examples: • Patterns of patient behavior for known issues • Drivers for high cost buckets	Examples: • Static data elements (e.g., address) used for linking regional behavior • Integration of rich case file information	Examples: • Compare various interventions for target populations • Measure simulated responses • Optimize interventions

Hybrid Approach
Proactively applies combination of all approaches at entity and network levels

RISK MODULES
ACTION AND RULES
PATIENT PROFILE
PREDICTIVE ANALYTICS
INTEGRATED DATA STORE

ANTICIPATORY
↑
PREDICTIVE
↑
REAL-TIME
↑
RETROSPECTIVE

'rear-view mirror'

SAS, Sep. 2015

GOAL: Maintain or improve the physical and psychosocial well-being of individuals through cost-effective and tailored health solutions.

Vulnerable **Digital** and **Virtual** Economy

"**Cyberwarfare** is **not something theoretical** or reserved for conflict in the distant future, but happening continuously right now… We're doing it all of the time. So is everybody else…"

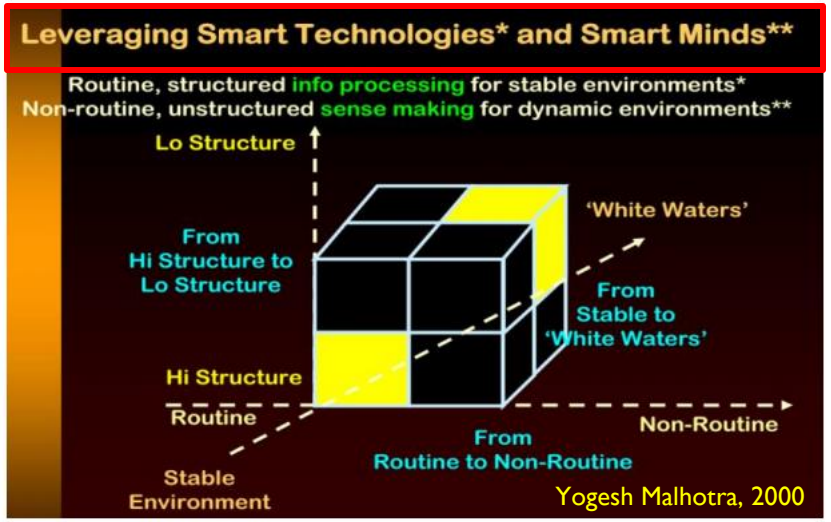
- Ability to incapacitate country's **power grids, 1994-**.
- Ability to disable **complete critical NII: banking**, railroads, airlines, sewage, water and electric power, **1999-**.

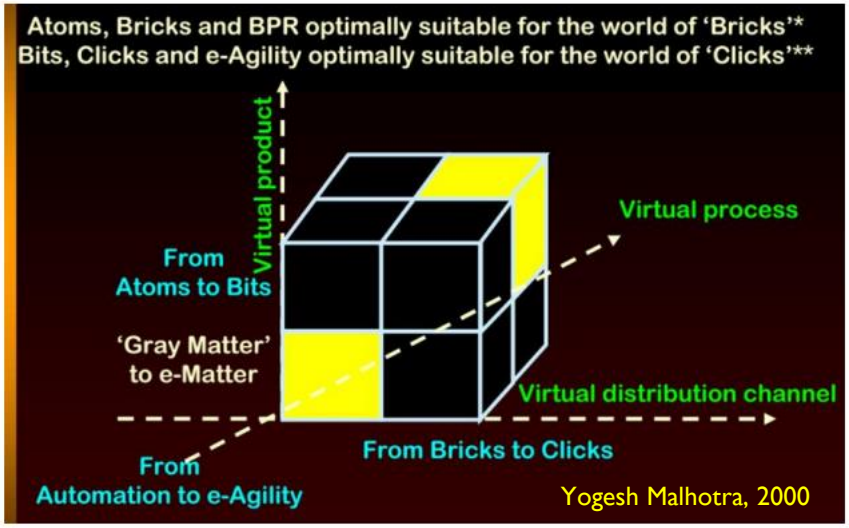
Finance is the **most information intensive industry** given that its products and services, processes, as well as channels of distribution and consumption are all digital.

- Global Financial Markets, Exchanges, & Trading Networks
- Global Transactions, Payments, & Money Transfer Networks

Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics http://ssrn.com/abstract=2553547

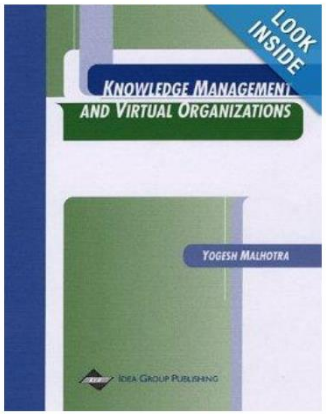
20-Years of **Digital Transformation** Models





DIGITIZATION-VIRTUALIZATION

2000



http://www.yogeshmalhotra.com/ModelRiskManagement.htm

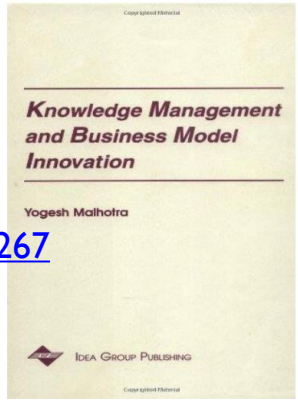
http://www.yogeshmalhotra.com/publications.html

http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=2338267

http://scholar.google.com/citations?user=MGblsfkAAAAJ

BUSINESS MODEL INNOVATION

2001



Toward Managing Catastrophic Risks

Risk, Uncertainty, and Profit for the Cyber Era: 'Knight Reconsidered'
http://ssrn.com/abstract=2553547

"Normality has been an accepted wisdom in economics and finance for a century or more. Yet in **real-world systems**, nothing could be less normal than normality. Tails should not be unexpected, for they are the rule… As the world becomes increasingly **integrated** – financially, economically, socially – **interactions** among the moving parts may make for potentially fatter tails....

... Catastrophe risk may be on the rise."

-- Andrew G Haldane, Executive Director, Financial Stability and member of the Financial Policy Committee and Benjamin Nelson, Economist, Financial Stability, Bank of England, in 'Tails of the unexpected' speech at "The Credit Crisis Five Years On: Unpacking the Crisis", 8 June 2012.

Modeling Catastrophic Risks

Extreme Value Theory (EVT): Theory of modelling and measuring extreme events, i.e., events which occur with very small probability.

- Example: Measurement of extreme losses i.e., left-tail, in P&L distribution.
- Extracts reliable measure of estimated loss given limited data for extreme event.

Two Fundamental Methods: Block Maxima and Point Over Threshold methods.

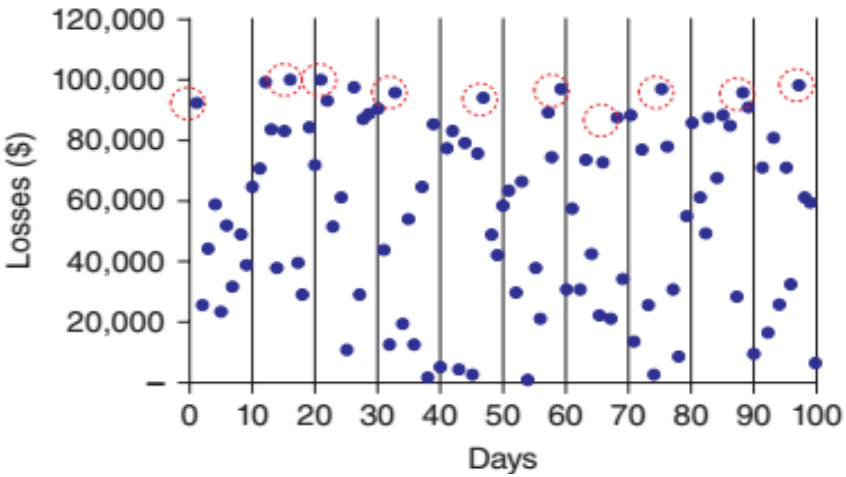
Block Maxima (BM) Method: Subdividing the time period of loss data into a set of equal blocks (sub-periods) and taking the **maximum loss in each block** gives the local block maxima. It can be used to characterize or fit a probability distribution and is often called **generalized extreme value (GEV) distribution**.

Peaks Over Threshold (POT) Method: More widely used method based on choice of a numerical threshold which denotes **every loss over the threshold** as extreme loss. It can be used to characterize or fit a probability distribution and is often called **generalized Pareto distribution (GPD)**.

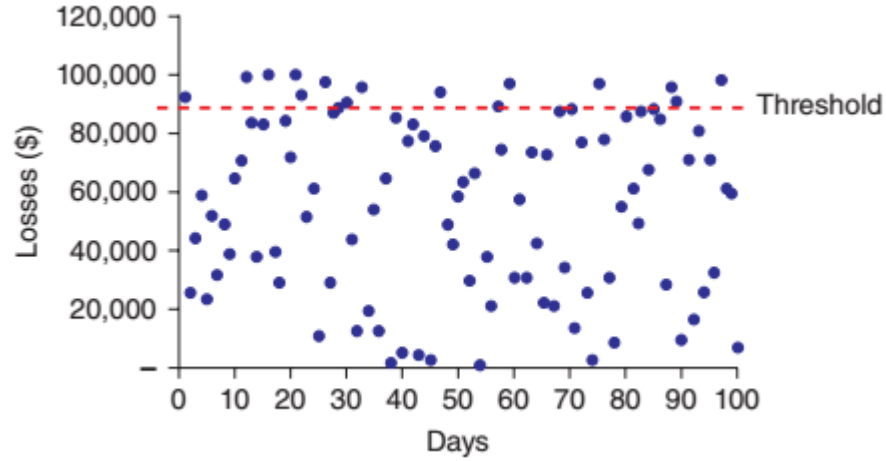
Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management
http://ssrn.com/abstract=2538401

Measuring & Managing Financial Risks with Improved Alternatives Beyond Value-at-Risk (VaR)
http://ssrn.com/abstract=2594859

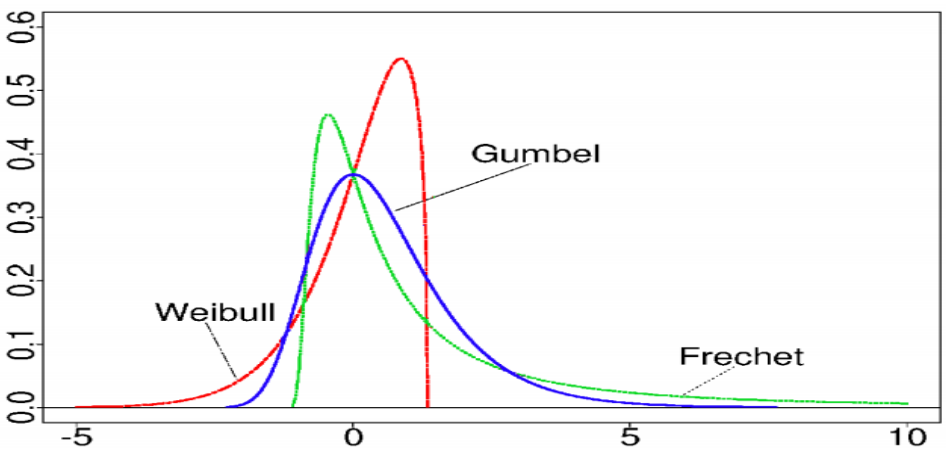
Block Maxima (BM) vs. Peaks Over Threshold (POT)

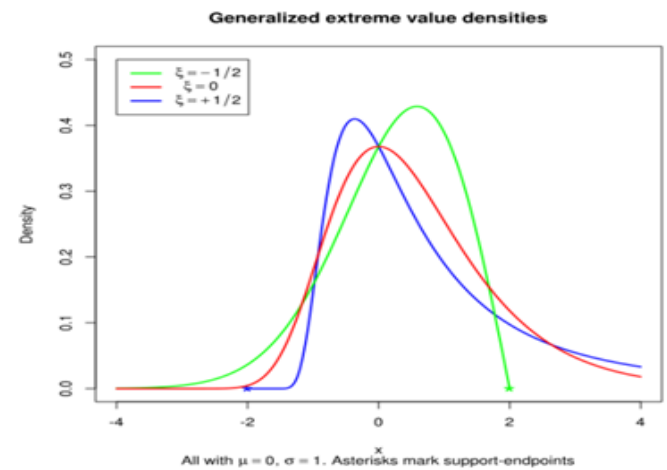


The largest losses in each 10-day block



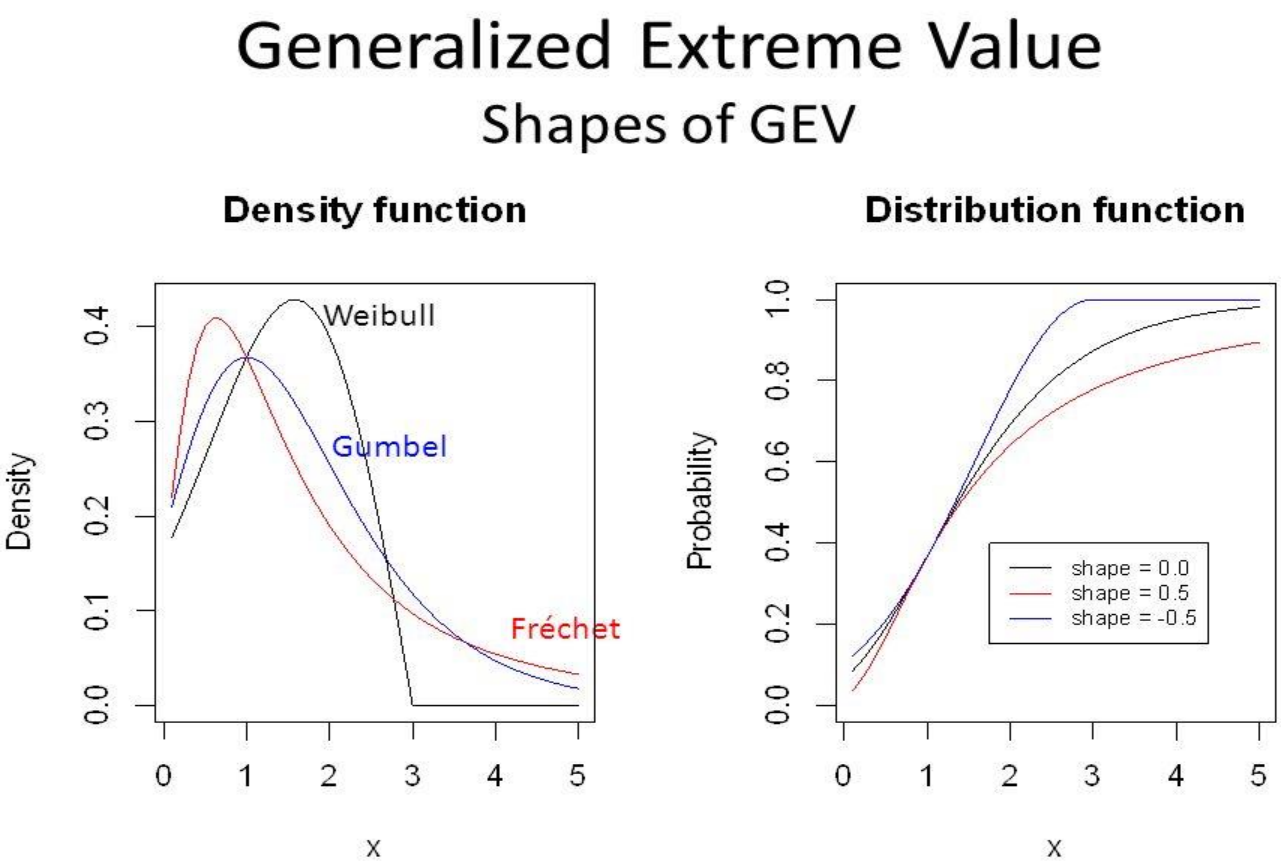
Losses over a threshold





http://www.darbyshirehampton.com/

Need for Extreme Value Methods… and Data



Shape parameter v defines several distributions:

Gumbel: $v = 0$

Weibull: $v < 0$

Fréchet: $v > 0$

CDF H(x)

Almost all common continuous distributions converge on $H(x)$ for some value of v

Weibull – beta

Gumbel – normal, lognormal, hyperbolic, gamma, chi-squared

Fréchet – Pareto, inverse gamma, Student t, loggamma

http://ssrn.com/abstract=2553547

Modeling Catastrophic Risks

- **Extreme Value Theory (EVT)**

GEV EVT distributions combine the 3 types.

GPD used for modeling tails of other distributions.

CDF $F(x) = P(X \leq x)$

CDF $F_u(y) = P(X - u \leq y \mid X > u)$

$y = X - u$, excess loss or exceedance over the threshold

for a reasonably high threshold, u, $F_u(y)$ ~ General Pareto Distribution (GPD)

$$G(X) = \begin{cases} 1 - \left(1 + \frac{\xi y}{\beta}\right)^{-1/\xi} & \textit{if } \xi \neq 0 \\ 1 - \exp\left(-\frac{y}{\beta}\right) & \textit{if } \xi = 0 \end{cases}$$

where $y = X - u$, $\xi = 1/\alpha$ shape parameter, α the tail index

β simple scaling parameter. **Parameters Estimation:**
maximum likelihood, elemental percentile method and the method of moments

http://www.darbyshirehampton.com/

Modeling Catastrophic Risks

VaR using the GPD approach

$$VaR_{1-\alpha} = u + \frac{\beta}{\xi}\left(\left(\frac{N}{n_u}\alpha\right)^{-\xi} - 1\right)$$

where N is the total number of data points
n_u the number of data points
that exceed the threshold u.

expected shortfall $ES_{1-\alpha}$ $\quad ES_{1-\alpha} = \frac{VaR_{1-\alpha}}{1-\xi}\frac{\beta - \xi u}{1-\xi}$

if amount of data in the tail of the returns distribution small
it leads to broad confidence intervals and weak significance estimates.
Both the BM and POT method suffer from the problem of limited data
although it is possible to reduce the time division in the BM
or lower the threshold for the POT
to produce more data points to fit to the desired distribution.

Modeling Catastrophic Risks

Generalized Pareto Distribution (GPD) for extreme tail of a wide range of distributions
EVT is concerned only with the tail of the distribution

As you let the threshold u go to infinity, distribution of observations beyond the threshold (call them y) converge to the $GPD(y;\xi,\beta)$, where

$$GPD(y;\xi,\beta) = \begin{cases} 1-(1+\xi y/\beta)^{-1/\xi} & \text{if } \xi > 0 \\ 1-\exp(-y/\beta) & \text{if } \xi = 0 \end{cases}$$

fat tails. Student's $t(d)$
normal distribution

with $\beta > 0$ and $y \geq u$.

We could use MLE to estimate the GPD distribution however, if $\xi > 0$

Hill estimator $F(y) = 1 - cy^{-1/\xi} \approx 1-(1+\xi y/\beta)^{-1/\xi} = GPD(y;\xi,\beta)$

conditional distribution $f(y|y>u) = f(y)/\Pr(y>u) = f(y)/(1-F(u))$, for $y > u$

$F(u) = 1 - cu^{-1/\xi}$

$$f(y) = \frac{\partial F(y)}{\partial y} = \frac{1}{\xi} c y^{-1/\xi - 1}$$

http://www.risklab.ch/

Modeling Catastrophic Risks

$$L = \prod_{i=1}^{T_u} f(y_i)/(1 - F(u)) = \prod_{i=1}^{T_u} \frac{1}{\xi} c y_i^{-1/\xi - 1} / (c u^{-1/\xi}), \quad \text{for } y_i > u$$

T_u is the number of observations y larger than u, rule of thumb set $T_u = 50$.

log-likelihood function is $$\ln L = \sum_{i=1}^{T_u} \left(-\ln(\xi) - (1/\xi + 1)\ln(y_i) + \frac{1}{\xi}\ln(u) \right)$$

Hill estimator Taking the derivative with respect to ξ and setting it to zero

$$\xi = \frac{1}{T_u} \sum_{i=1}^{T_u} \ln(y_i/u)$$

c parameter $F(u) = 1 - cu^{-1/\xi} = 1 - T_u/T$ Solving for c, $c = \frac{T_u}{T} u^{1/\xi}$

estimate of the cumulative density function for observations beyond u

$$F(y) = 1 - cy^{-1/\xi} = 1 - \frac{T_u}{T}(y/u)^{-1/\xi}$$

http://www.actuaries.org/ASTIN/Colloquia/Helsinki/Presentations/Embrechts.pdf

CRITICALLY NEED SMART MINDS for applying SMART TECHNOLOGIES

Dear Sir

The article "Of couples and copulas", published on 24 April 2009, suggests that David Li's formula is to blame for the current financial crisis. For me, this is akin to blaming Einstein's $E=mc^2$ formula for the destruction wreaked by the atomic bomb.

Feeling like a risk manager whose protestations of imminent danger were ignored, I wish to make clear that many well-respected academics have pointed out the limitations of the mathematical tools used in the finance industry, including Li's formula. However, these warnings were either ignored or dismissed with a desultory response: "It's academic".

We hope that we are listened to in the future, rather than being made a convenient scapegoat.

Yours Faithfully,
Professor Paul Embrechts
Director of RiskLab
ETH Zurich

Also Harry Panjer

Additional Models and References

- Bayesian and Quasi-Bayesian VaR
- Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management http://ssrn.com/abstract=2538401
- Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics http://ssrn.com/abstract=2553547
- Bayesian Inference: Bayesian Nets & Credal Nets
- Possibility Theory: Fuzzy Sets
- Quantum Computing
- Beyond Model Risk Management to Model Risk Arbitrage for Fintech Era: How to Navigate 'Uncertainty'... When 'Models' are 'Wrong'... And 'Knowledge'... 'Imperfect'! http://ssrn.com/abstract=2766099

"The **new business model** of the Information Age, however, is marked by **fundamental, not incremental, change**. Businesses **can't plan long-term**; instead, they **must shift** to a more flexible **"anticipation-of-surprise" model**."
-- Dr. Yogesh Malhotra in ***CIO Magazine*** interview, Sep. 15, 1999.

CIO

Advancing Beyond 'Predictive' to 'Anticipatory' Risk Analytics

CyberFinance: Why Cybersecurity Risk Analytics must Evolve to Survive 90% of Emerging Cyber Financial Threats, and, What You Can Do About It?

1. 20-Years of Anticipatory Risk Analytics
2. *Griffiss Cyberspace*™ and Cyber 9-11
3. RSA1024 'Gold Standard' Shattered
4. Mis-measure of Cyber Risk @ CERT
5. Cyber Risk Industry Mis-measure of Risk
6. Cyber déjà vu of Global Financial Crisis
7. Global Cyber Insurance Crisis Averted
8. Materiality of Cyber Risk, Lack Thereof
9. The Cyber-Finance-Trust Framework
10. Beyond Mis-measure of Cyber Risk
11. The 'Iceberg' of Cyber-Finance Risk
12. '*Uncharted Territories*' of Cyber-Finance
13. Beyond Risk to Managing Uncertainty
14. Beyond NHST-Determinism to Bayesian
13. Bayesian & Markov Chain Monte Carlo
14. Increasingly Vulnerable Time and Space
15. Vulnerable Digital & Crypto-Currencies
16. 20-Years of Digital Transformation Models
17. Exponentially Growing Vulnerabilities
18. Black Hat Finance of FinTech Models
19. Assume Breach & Crypto-Apocalypse
20. Healthcare More Vulnerable than Finance?
21. Healthcare: Following Finance Analytics?
22. Vulnerable Digital and Virtual Economy
23. Toward Managing Catastrophic Risks
24. Modeling Catastrophic Risks
25. Additional Models and References

Beyond 'Predictive' to 'Anticipatory' Risk Analytics

'What gets measured, gets managed.' – Peter Drucker

Yogesh Malhotra's Analytics Corollaries:

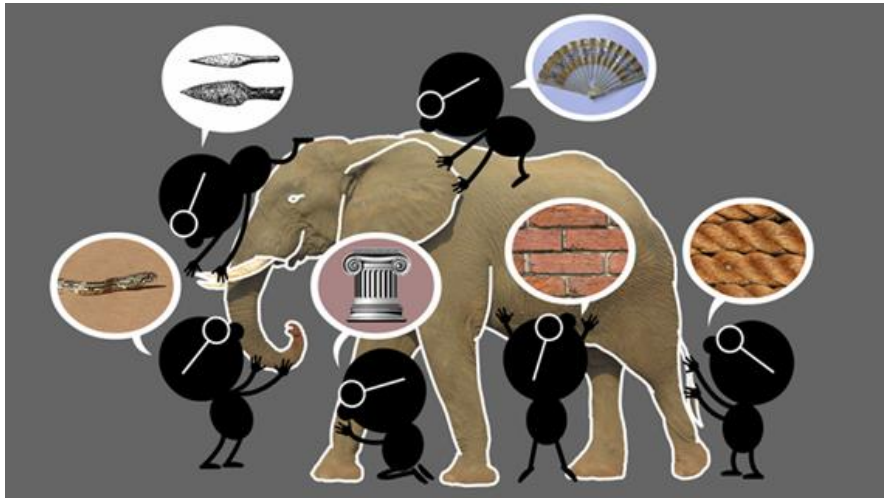
'On the folly of rewarding A, while hoping for B' – Steve Kerr

What gets mismeasured, gets mismanaged.

What gets mostly mismeasured, gets mostly mismanaged.

Two Guiding Questions on *Prediction*: IT, Statistics, Controls.

"Driving forward by looking through the rear-view mirror..."
- ISR's description of the IS field, 1993



"**Models are backward-looking**." – Wall Street CEOs after the 'Crisis' of 2008-2009

References: Recent Research

- Risk, Uncertainty, and Profit for the Cyber Era: 'Knight Reconsidered'

- Beyond Model Risk Management to Model Risk Arbitrage for Fintech Era
- Future of Finance Beyond 'Flash Boys': Risk Modeling for Managing Uncertainty
- Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management
- Markov Chain Monte Carlo Models, Gibbs Sampling, & Metropolis Algorithm
- Cybersecurity & Cyber-Finance Risk Management: Threats & Vulnerabilities
- Measuring & Managing Financial Risks with Improved Alternatives beyond VaR
- A Risk Management Framework for Penetration Testing of VoIP Protocols
- Quantitative Modeling of Mobile Trust and Trust Management Protocols
- Number Field Sieve Cryptanalysis Algorithms for Prime Factorization

http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=2338267

"The **new business model** of the Information Age, however, is marked by **fundamental, not incremental, change**. Businesses **can't plan long-term**; instead, they **must shift** to a more flexible **"anticipation-of-surprise" model**."
-- Dr. Yogesh Malhotra in ***CIO Magazine*** interview, Sep. 15, 1999.

CIO

Anticipatory Risk Analytics: Growing Awareness

SANS

"Organizations need anticipatory, active defenses designed to frustrate, annoy and deceive advanced **adversaries** (and **insiders**) who have already achieved access to their innermost sanctums." – SANS Institute October 6, 2015, *InfoSecurity Magazine*
To Stop APTs You Need Anticipatory Active Defenses

RSA

"Data drives decision making for people and computer systems. When that data is unknowingly [**or knowingly**] manipulated, those decisions will be made based on false data.... The advent of connected and automated sensors aggressively exacerbates these issues."
– RSA, Dec. 10, 2015, SiliconAngle NewsLetter

CGI

"The other aspect is digital transformation and the computerization of everything. .. One of the key things in cybersecurity is not just about there being more bad guys out there, but that the different kinds of cyber and information technology entry points are growing [**exponentially**] all the time." – Homeland Preparedness News, May 27, 2016

20-Years Leading Global Research & Practices in Advancing Beyond 'Predictive' to 'Anticipatory' Risk Analytics

http://FinRM.org/

19th New York State Cyber Security Conference Presentation, Albany, NY
June 8 - 9, 2016, Empire State Plaza - Albany, NY

CyberFinance: Why Cybersecurity Risk Analytics must Evolve to Survive 90% of Emerging Cyber Financial Threats, and, What You Can Do About It?

Advancing Beyond 'Predictive' to 'Anticipatory' Risk Analytics

Yogi

Dr. Yogesh Malhotra
PhD, MSQF, MS-CS, MS-NCS, MS-Acc, MBA-Eco, C.Eng., CISSP, CISA, CEH, CCP/CDP
Who's Who in America®, Who's Who in the World®,
Who's Who in Finance & Industry®,
Who's Who in Science & Engineering®
www.yogeshmalhotra.com
dr.yogesh.malhotra@gmail.com

www.its.ny.gov

FinRM™
Global Risk Management Network, LLC,
757 Warren Rd, Cornell Business & Technology Park, Ithaca, NY 14852-4892
Phone: 646-770-7993

"The **new business model** of the Information Age, however, is marked by **fundamental, not incremental, change**. Businesses **can't plan long-term**; instead, they **must shift** to a more flexible **"anticipation-of-surprise" model**."
-- Dr. Yogesh Malhotra in ***CIO Magazine*** interview, Sep. 15, 1999.

CIO